

**UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO**

FACULTAD DE DERECHO

**“EL CHEQUE ELECTRÓNICO, SU IMPORTANCIA Y
NECESIDAD ACTUAL DE REGULACIÓN EN MÉXICO”**

T E S I S

QUE PARA OPTAR AL TÍTULO DE:

LICENCIADO EN DERECHO

P R E S E N T A

FERNANDO OLVERA VARGAS

ASESOR. DR. GERARDO RODRÍGUEZ BARAJAS

CIUDAD UNIVERSITARIA

2011



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Para mi Dios, al Todopoderoso, al Alfa y la Omega,
al Señor de los ejércitos, al Señor de señores.
Para mi Padre, mi Creador,
a Jesucristo, su hijo unigénito, mi Salvador, y
al Espíritu Santo, mi Protector.
A ti mi Señor sea la gloria.
Amén.

A mis papás, porque sin ustedes
no estaría aquí.
Gracias papá y mamá.

A mi esposa, por tu fidelidad.

A mis hijos Fer, Moises y Sara (que viene
en camino), por su inocencia.

A mis hermanos Jennie y Chris,
y cuñado Horacio, por su apoyo incondicional.

A mis suegros y cuñados, por su confianza.

A mis tíos(as), primos(as), sobrinos(as), de quienes anhelo
sean prosperados(as) en todo.

A mis pastores y líderes, por doblar su rodilla
en oración.

A mis autoridades laborales, las presentes y las que en
la trayectoria laboral he tenido, por su tenacidad y perseverancia.

A mi asesor, por su paciencia e instrucción en el desarrollo de la presente tesis profesional.

A todos aquellos(as) que de alguna forma me han apoyado.

A todos aquellos que hacen el bien.

ÍNDICE

Introducción.

Lista de abreviaturas y siglas.

Capítulo Primero

El comercio electrónico

1. Aspectos fundamentales	1
1.1. Concepto y alcances del comercio electrónico	1
1.2. Tipos de comercio electrónico	6
1.3. El derecho informático	8
1.3.1. Nociones básicas	8
1.3.2. Características fundamentales	9
1.3.3. Informática jurídica	10
1.3.4. Derecho de la informática	16
1.3.5. Gobierno digital y ciberjusticia	37
1.3.6. Delitos informáticos	42
1.3.7. Aplicación actual en México	57
1.4. Medios de comunicación	76
1.5. Medios electrónicos	77
1.5.1. Internet	77
1.5.2. Télex	79
1.5.3. Telégrafo	79
1.5.4. Correo electrónico	80
1.5.5. Intercambio electrónico de datos (EDI)	81
1.5.6. Fax	82
1.5.7. Medios ópticos o similares	83
1.6. Ley Modelo sobre el Comercio Electrónico de la CNUDMI	83
1.7. Equivalencia funcional	96
2. Aplicaciones del comercio electrónico	101
2.1. Utilidad en la práctica y ventajas	101
2.2. Medios de pago electrónico (EPS)	106
2.3. El dinero electrónico	110
2.4. La transferencia electrónica	112
2.5. Comercio electrónico marítimo	117
2.6. Cuestiones de la fiscalidad en relación con el comercio electrónico	119

3. El comercio electrónico en México, y derecho comparado	124
3.1. Regulación del comercio electrónico en México	126
3.2. Situación actual del comercio electrónico en España	133
3.3. Normativa Colombiana sobre comercio electrónico	144
4. Los mensajes de datos	160
4.1. Concepto	160
4.2. Partes	161
4.3. Identidad del emisor	163
4.4. Momento de expedición	166
4.5. Lugar de expedición y recepción	167
4.6. Momento de la recepción	167
4.7. Acuses de recibo	169
4.8. Contratos mercantiles celebrados por mensajes de datos	172
4.9. Valor probatorio a los mensajes de datos	175
4.10. Conservación de mensajes de datos	178
4.11. El mensaje de datos en el Código de Comercio	180

Capítulo Segundo

Firma electrónica

1. Ley Modelo de la CNUDMI sobre las Firmas Electrónicas	184
2. Tipos de firma electrónica	191
2.1. Firma electrónica simple (FE)	192
2.2. Firma digital	194
2.3. Firma electrónica avanzada (FEA/FIEL)	195
3. Firma electrónica avanzada (FEA/FIEL)	197
3.1. Concepto	197
3.2. Confiabilidad de la firma electrónica avanzada	197
3.3. Certificación	198
3.4. Cómo se firma un documento digital	200
3.5. Diferencias entre firma electrónica y FEA(FIEL)	201
3.6. La firma electrónica avanzada como requisito del elemento formal en los actos jurídicos	202
3.7. Elementos que participan en la FEA(FIEL)	204
3.8. Requisitos de seguridad de la FEA(FIEL)	208
3.9. Proceso para implementar la FEA(FIEL)	209
3.10. Alcance y valor probatorio de documentos con FEA(FIEL)	210
3.11. La FEA(FIEL) en materia fiscal	213
3.12. Certificado digital	215
3.13. Sello digital	219
4. Prestadores de servicios de certificación en materia mercantil	222
4.1. Requisitos para obtener acreditación como PSC	223
4.2. Acreditación de los PSC conforme al reglamento del Código de Comercio en materia de PSC	224
4.3. Certificado de acreditación como PSC	226

4.4. Contratos de certificación de autoridad	227
4.5. Certificados digitales en materia mercantil	228
4.6. Contenido del Certificado digital en materia comercial conforme al Código de Comercio	229
4.7. El certificado conforme al Reglamento del Código de Comercio en materia de PSC	230
4.8. Obligaciones de los PSC en la FEA(FIEL)	231
4.9. Obligaciones del titular del certificado	233
4.10. Del reconocimiento de certificados y firmas electrónicas extranjeras	234
5. Criterio e interpretación actual del Código de Comercio sobre la firma electrónica, y derecho comparado	235

Capítulo Tercero

El cheque electrónico

1. Concepto. ¿Forma especial del cheque o un nuevo cheque?	244
2. Naturaleza y elementos	245
3. Presupuestos	253
4. Diferencias entre cheque electrónico y transferencia electrónica	255
5. Forma de uso del cheque electrónico en México	259
6. Funcionamiento, práctica y utilidad actual del cheque electrónico como medio de pago en Estados Unidos de América	259
7. Importancia y necesidad de implementar y regular el cheque electrónico como medio de pago en México	263
8. Propuesta de reforma al Código de Comercio y a la Ley General de Títulos y Operaciones de Crédito	268

Glosario

Conclusiones.

Bibliografía.

LISTA DE ABREVIATURAS Y SIGLAS

ABA	Asociación Americana de la Barra de Abogados
ABM	Asociación de Banqueros de México
AC	Autoridad Certificadora
ACLU	–siglas en inglés- Asociación de Libertades Civiles de Estados Unidos
AMECE	Asociación Mexicana de Estándares para el Comercio Electrónico
AMIPCI	Asociación Mexicana de Internet
AMITI	Asociación Mexicana de la Industria de Tecnologías de Información
ARC	Autoridades Certificadoras Centrales
ARPANET	Advanced Research Agency Network
@ECE	Asociación Española de Comercio Electrónico
B2A	Bussines to Administration
B2B	Bussines to Bussines
B2C	Bussines to Consumer
B2G	Bussines to Government
CCITT	Comité Consultivo Internacional Telegráfico y Telefónico
CFA	Comité de Asuntos Fiscales
CIEC	Clave de Identificación Electrónica Confidencial
CIF	Costo, seguro, fletes.
CLI	Cyberspace Law Institute
CMD	Mead Data Central
CNUMI	Comisión de Naciones Unidas para el Derecho Mercantil Internacional
CPR	–siglas en ingles- Instituto para la Resolución de Conflictos
CRDP	Centre de Recherche en Droit Publique
CTIC	Centro Tecnológico de la Información y Comunicación
e-administración	administración electrónica
e-business	negocio electrónico

e-Cash	–siglas en inglés- dinero electrónico
e-democracia	democracia electrónica
e-gobierno	gobierno electrónico
e-government	gobierno electrónico
e-mail	correo electrónico
e-Resolution	resolución electrónica
e-shop	tienda electrónica
EDI	Electronic Data Interchange
EPS	–siglas en inglés. Medios de Pago Electrónico.
ERP	–siglas en inglés- Planificación de Recursos Empresariales
FE	Firma Electrónica
FEA/FIEL	Firma Electrónica Avanzada
GICE	Grupo Impulsor del Comercio Electrónico
HLC	Health Law Center
IANA Internet	Assigned Numbers Authority
ICANN	–siglas en inglés- Corporación de Internet para la Asignación de Nombres y Números
IEN	Instituto de Estadística de Navarra
IFCAI	–siglas en inglés- Federación Internacional de Instituciones de Arbitraje Comercial (IFCAI)
INAPAM	Instituto Nacional de Personas Adultas Mayores
INTERNET	Interconnected networks
IVA	Impuesto al Valor Agregado
INEGI	Instituto Nacional de Estadística y Geografía
LAN	Red de Área Local
NACPEC	-siglas en inglés- Proyecto Norteamericano sobre Protección al Consumidor en Comercio Electrónico
NAF	–siglas en inglés- Foro de Arbitraje Nacional
NCAIR	National Center for Automated Information Research
NICS	–siglas en inglés- Red de la Policía Internacional
NIP	Número de Identificación Personal
OBAR	Corporación de Investigación Automatizada de la Barra de

Ohio	
OCDE	Organización para la Cooperación y el Desarrollo Económico
OMC	Organización Mundial del Comercio
OMPI	Organización Mundial de la Propiedad Intelectual
ONTSI	Observatorio Nacional de Telecomunicaciones y de la Sociedad de la información
PSC	Prestadores de Servicios de Certificación
PKI	Public Key Infrastructure
RSA	Rivest, Shamir y Adleman
SAT	Sistema de Administración Tributaria
SE	Secretaría de Economía
SET	Secure Electronic Transaction
SITA	Red de la Sociedad Internacional de Telecomunicaciones Aeronáuticas
SISE	Sistema Integral de Seguimiento de Expedientes
SPAM	Shoulder Pork and hAM/SPiced hAM
SPEI	Sistema de Pagos Electrónicos Interbancarios
SSL	Secure Socket Layer
SWIFT	–siglas en inglés- Red Bancaria de Intercambio de Mensajes Financieros
TIC	Nuevas Tecnología de Información y Comunicación
UNCTC	–siglas en inglés- Centro de Corporaciones Transnacionales de las Naciones Unidas
UNCTAD	–siglas en inglés- Comisión de Comercio y Desarrollo de las Naciones Unidas
UE	Unión Europea
WWW	World Wide Web

INTRODUCCIÓN

Es indudable que existe la importancia de renovar el pensamiento y mirar hacia la unificación de un modelo económico, que aborde la solución contra la desigualdad económica; la condición: “mirar hacia adelante”.

Tener la visión de desarrollo global a través de la apertura económica, en donde la utilización de las nuevas tecnologías de información y comunicación (TIC), juegan un papel importante.

Cabe destacar que actualmente se ha incrementado la utilización de las tecnologías. Desde el campo económico hasta el cultural, la tecnología ha representado importantes cambios de desarrollo, aparejado con el surgimiento de nuevos conceptos, entre otros, a saber: gobierno (gobierno electrónico); administración (prestación de servicios públicos por Internet); democracia (voto electrónico); jurisdiccional (ciberjusticia, juicios en línea, expediente electrónico); derecho (informática jurídica, derecho de la informática); educación, información, comunicación, cultura (Internet, correo electrónico); operaciones fiscales (firma electrónica avanzada); comercio marítimo (conocimientos de embarque electrónico, documentos de transporte multimodal); laboral (ergonomía, teletrabajo); medios probatorios (mensajes de datos).

Internet, considerado como un acontecimiento informático, resulta un elemento clave que genera desarrollo no únicamente en la esfera económica; sino, además en la apertura de información y comunicación en el mundo.

En México se ha legislado sobre la utilización de Internet, entre algunos ordenamientos se encuentran: Código Federal de Procedimientos Civiles, Código Fiscal de la Federación, Ley del Servicio de Tesorería de la Federación, Ley de Obras Públicas y Servicios Relacionados con las Mismas, Ley Federal de Procedimiento Administrativo, Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, Código Federal de Instituciones y Procedimientos

Electoral, Código Federal de Procedimientos Penales, Ley de Coordinación Fiscal, Ley de Fiscalización y Rendición de Cuentas de la Federación, Ley de Instituciones de Crédito, Ley de la Policía Federal, Ley de Petróleos Mexicanos, Ley del Mercado de Valores, Ley del Servicio de Administración Tributaria, Ley Federal de Extinción de Dominio, Ley General de Bienes Nacionales, Ley de Educación del Distrito Federal, y Ley para Prevenir y Erradicar la Trata de Personas, el Abuso Sexual y la Explotación Sexual Comercial Infantil para el Distrito Federal.

Asimismo, se ha creado la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que regula el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal, así como la protección de los datos personales.

En materia jurisdiccional, nace el “Juicio en Línea”, regulado en la Ley Federal de Procedimiento Contencioso Administrativo, en el que se establece que el juicio contencioso administrativo federal se promoverá, substanciará y resolverá en línea, a través del Sistema de Justicia en Línea que deberá establecer y desarrollar el Tribunal Federal de Justicia Fiscal y Administrativa; su inicio, en agosto de 2011.

Entre las oportunidades que en materia mercantil generan las tecnologías de información y comunicación, se encuentra, la compra y venta electrónica de bienes y servicios, llamado “comercio electrónico”. En esta nueva modalidad, se realizan negocios electrónicos, a través de una economía digital, aparejado con una estrategia de marketing electrónico, y cuyas formas de pago, son por medio de dinero electrónico o banca electrónica.

En esa tesitura, México ha tomado la decisión legislativa de reformar diversos ordenamientos legales, en base a la Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico, y a la Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional sobre Firmas Electrónicas.

El 29 de abril de 2000 se aprobaron reformas al Código de Comercio, Código Civil Federal, Ley Federal de Protección al Consumidor, y al Código Federal de Procedimientos Civiles. Más adelante, el 29 de agosto 2003, nuevamente se reforma el Código de Comercio, y se da reconocimiento a la firma electrónica avanzada; y, en 2009, en el mismo ordenamiento mercantil, se publican reformas relativas a las garantías mobiliarias.

A través de Internet fluye información alrededor del mundo, que puede ser susceptible de ser leída, copiada, retransmitida, usada o editada por personas ajenas a los autores, destinatarios o emisores; de ahí, nace la Firma Electrónica Avanzada, la cual ha sido adoptada como instrumento de seguridad sobre la autenticación, confidencialidad e integridad de la información, en donde interviene el proceso de encriptación. De esa forma, la firma electrónica avanzada es utilizada como mecanismo de seguridad para identificar al firmante en relación con un mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

Bajo esos elementos, se propone el cheque electrónico, el cual, técnicamente, es un mensaje de datos. Formalmente, es un título valor con fines de instrumento de pago, en donde la provisión se encuentra garantizada, y cuya cualidad de fiabilidad es respaldada por la firma electrónica avanzada.

Es un documento electrónico que en mucho rebasa al cheque sobre papel, el cual si bien este ha significado un medio de pago en el mundo desde mediados del siglo XVIII, también lo es que, ha representado costos elevados para los bancos, en cuanto al proceso de cobro y devolución, a lo que se añade el impacto ambiental por el uso de papel, su susceptibilidad de robo y/o extravío, que conlleva la fácil falsificación de la firma del librador, y la inseguridad que representa su cobro por la falta de provisión cuando no es certificado.

El balance indica un avance en la tendencia global en las relaciones

comerciales a través de las nuevas tecnologías de información y comunicación, donde en cada gobierno existe la responsabilidad de llevar a cabo el estudio de estas nuevas tecnologías, así como su aplicación, que conduzcan a una integración de la economía en el mundo. No podemos dejar de avanzar, sino renovar nuestra mente, y lo que hoy impera mundialmente, es el “fenómeno globalizador”, del cual puede sacarse el mayor provecho: “Retener lo bueno y desechar lo malo”.

La tecnología representa nuevas formas de perfeccionamiento, estimula la visión de progreso y trasciende a nuevos retos; cuyo propósito, es alcanzar el desarrollo, innovación y renovación de un país.

La meta, buscar un sentido de cooperación internacional, y dirigir los esfuerzos a nuevas oportunidades que alcancen a todas las naciones, a mejores condiciones de vida.

Sin duda, la tecnología es una herramienta que, utilizada para el bien, impacta de manera total una nación.

Confío que un día el hombre alcance el propósito bueno, agradable y perfecto por el que fue creado.

Capítulo Primero

El comercio electrónico

1. Aspectos fundamentales.

1.4. Concepto y alcances del comercio electrónico

Es fundamental para toda nación, empresa, sociedad, familia y cada persona, dentro de un fenómeno globalizador, ser punta de lanza; ser cabeza y no cola; siempre ir más allá; no conformarse con lo que ofrece el mundo, sino, crear, innovar, mirar siempre hacia adelante.

Presenciamos nuevos cambios en todos los ámbitos; nuevos pensamientos, nuevos proyectos, nuevas estructuras, nuevos gobiernos, nuevas estrategias, nuevas economías, nuevas formas de comercio.

Desde las primeras maneras de ofrecer un producto, como fueron las “ferias de Champagne en 1265”¹, “que atraían comerciantes de muy remotas regiones”², hasta llegar actualmente a la nueva modalidad de comercio llamada: comercio electrónico, se advierte que el comercio ha evolucionado, derivado de las “innovaciones desarrolladas en el ámbito de las técnicas mercantiles.”³

En esa tesitura, cabe mencionar la importancia del comercio electrónico, dada su trascendencia económica, política, social y jurídica, que provoca la actualización a los regímenes jurídicos nacionales e internacionales, en un ambiente de seguridad y confiabilidad, que cuente con un respaldo jurídico uniforme, y que sea acorde a las tendencias de cambio.

¹ Valdeón, Julio, *La Baja Edad Media*, Red Editorial Iberoamericana, Sociedad Anónima (REI- México), México, 1988, pág. 16.

² Mantilla Molina, Roberto L., *Derecho Mercantil*, editorial Porrúa, Sociedad Anónima de Capital Variable, Décimo Cuarta reimpresión, México 2007, pág. 6.

³ Ídem.

Por ello, para entrar al estudio del comercio electrónico, es sustancial tener una concepción de éste, que integre los elementos que lo componen.

El comercio electrónico es la actividad comercial, que comprende transacciones de bienes y servicios, así como el flujo de información, a través de medios electrónicos.

Los autores Joan Hortalà i Vallvé, Franco Roccatagliata y Piergiorgio Valente, dan diversos conceptos sobre comercio electrónico, a saber:

“Desde las de las comunicaciones, el comercio electrónico consiste en la distribución de la información, productos servicios, transacciones financieras, a través de Redes de Telecomunicación Multimedia/Multiservicios, alineando sistemas de información de modo que se conformen nuevas estructuras empresariales de carácter virtual”.

“Desde la de los procesos de negocio, el comercio electrónico consiste en la utilización de tecnologías que faciliten el soporte y la automatización de los flujos de trabajo y procedimientos de negocio de la empresa, consiguiendo eficiencias en los costes, mejora la calidad de los servicios y acortando el tiempo de los ciclos de los procesos”.

“Desde la temporalidad, el comercio electrónico es el instrumento que permite establecer nuevos canales y nuevos mercados para el intercambio de productos, servicios e informaciones en tiempo real”.⁴

La doctora Judith Cavazos Arroyo y la maestra Soraya Reyes Guerrero, definen el comercio electrónico como: **“las transacciones que se realizan en línea, soportada por una serie de tecnologías que utilizan las computadoras y telecomunicaciones, las cuales facilitan el flujo de información”.**⁵

⁴ Joan Hortalà i Vallvé, Franco Roccatagliata y Piergiorgio Valente, *La fiscalidad del comercio electrónico*, Editorial CISS, Sociedad Anónima, Primera edición, Bilbao, 2000, p.p. 23.

⁵ Cavazos Arroyo, Judith y Reyes Guerrero, Soraya, *Comercio electrónico: un enfoque de modelos de negocio*. editorial Grupo Editorial Patria, Sociedad Anónima de Capital Variable, Primera reimpresión, México, 2008, p.p. 210.

El autor Miguel Ángel Davara Rodríguez, define el comercio electrónico, **“tanto la compra de productos o servicios por Internet, como la transferencia electrónica de datos entre operadores de un sector en un mercado, o el intercambio de cantidades o activos entre entidades financieras, o la consulta de información, con fines comerciales, a un determinado servicio, o un sin fin de actividades similares características realizadas por medios electrónicos”**.⁶

El escritor Nelson Remolina Angarita, Abogado y Especialista en Derecho Comercial, Profesor de la Facultad de la Universidad de los Andes, señala respecto del comercio electrónico, **“se refiere a todas las transacciones comerciales realizadas o basadas en sistemas electrónicos de procesamiento y transmisión de información, especialmente EDI (*Electronic Data Interchange*) e Internet (*Interconnected networks*)”**.⁷

Por su parte, la autora María Clara Gutiérrez Gómez, Abogada y Miembro de la Comisión Redactora de la Ley 527 de 1999, en Colombia, egresada de la Universidad de los Andes, define el comercio electrónico como: **“una modalidad mercantil que busca agilizar las relaciones comerciales existentes entre personas que se encuentran distantes”**.⁸

Asimismo, el investigador Julio Téllez Valdés, del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, primero define el “comercio” como: **“una serie cada vez mayor de actividades que tienen lugar en redes abiertas –compra, venta, comercio, publicidad, transacciones de toda índole- que conducen a un intercambio de valores entre las partes; luego, conceptúa el término “electrónico” como “la infraestructura mundial de tecnologías y redes de la informática y las telecomunicaciones que permiten el**

⁶ Davara Rodríguez, Miguel Ángel, *Manual de Derecho Informático*, editorial Arazandi, Sociedad Anónima, Séptima edición, Navarra, 2005, p.p. 197.

⁷ Universidad de los Andes, Facultad de Derecho, Internet, *Comercio Electrónico & Telecomunicaciones*, Legis Editores Sociedad Anónima, Primera edición, Colombia, 2002, p.p. 6.

⁸ *Ibidem*, p.p.176.

procesamiento y la transmisión de datos digitalizados”.⁹ En esa tesitura, define dicho autor al comercio electrónico, **“como cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como Internet”.**¹⁰

Por otra parte, los autores Soyla H. León Tovar, Hugo González García y Óscar Vázquez del Mercado Blanco, lo definen como **“el conjunto de actos de intermediación de bienes y servicios a través de mensajes de datos, transmitidos por medios electrónicos, ópticos o similares (internet, correo electrónico, intercambio electrónico de datos, facsímil, telegrama, o télex)”.**¹¹

De igual manera, los autores Charles E. McLure, Jr. y Giampaolo Corabi, definen al comercio electrónico como: **“el uso de la red informática para facilitar las transacciones que involucran la producción, la distribución, la venta y la entrega de bienes y servicios dentro del mercado”.**¹²

La OCDE (Organización para la Cooperación y el Desarrollo Económico), por su parte, define al comercio electrónico, como el proceso electrónico tanto previo a la negociación, como al funcionamiento y el proceso posterior de las transacciones de negocio entre los sujetos comerciales.¹³

En la Comunicación (97) 157, de la Comisión de las Comunidades Europeas, al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre Iniciativa Europea de Comercio Electrónico, de dieciséis de abril de mil novecientos noventa y siete, establece en su capítulo uno, un concepto de comercio electrónico, a saber: **“El comercio electrónico consiste en realizar electrónicamente transacciones comerciales. Está basado en el tratamiento y transmisión electrónica de datos, incluidos textos, imágenes y video. El comercio**

⁹ Téllez Valdés Julio, *Derecho Informático*, editorial Mc Graw-Hill/Interamericana Editores, Sociedad Anónima de Capital Variable, Cuarta edición, México, 2009, p.p. 214.

¹⁰ *Ibidem*, p.p. 218.

¹¹ León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, *La firma electrónica avanzada*, Oxford University Press México, Sociedad Anónima de Capital Variable, México, 2007, p.p. 25.

¹² Charles E. McLure, Jr. y Giampaolo Corabi, *La tributación sobre el comercio electrónico: objetivos económicos, restricciones tecnológicas y legislación tributaria*, Ediciones Depalma, Argentina, 2000, pág. 13.

¹³ www.ocde.com

electrónico comprende actividades muy diversas, como comercio electrónico de bienes y servicios, suministro en línea de contenidos digitales, transferencia electrónica de fondos, compraventa electrónica de acciones, conocimientos de embarque electrónicos, subastas, diseños y proyectos conjuntos, prestación de servicios en línea (*on line sourcing*), contratación pública, comercialización directa al consumidor y servicios posventa. Por otra parte, abarca a la vez productos (p.ej., bienes de consumo, equipo médico especializado) y servicios (p.ej., servicios de información, financieros y jurídicos), actividades tradicionales (p.ej., asistencia sanitaria, educación) y nuevas actividades (p.ej., centros comerciales virtuales)”¹⁴

En esa tesitura, se ha concluido que el concepto de comercio electrónico va más allá de lo que es la compra y venta electrónica de bienes, información o servicios; en virtud de que incluye otros actos y actividades como: la publicidad, la búsqueda de información acerca de productos, proveedores, negociación entre comprador y vendedor sobre precio, ofertas, contraofertas, condiciones de entrega, atención e información al cliente antes y después de la venta, logística, cumplimiento de trámites administrativos relacionados con la actividad comercial, colaboración entre empresas con negocios comunes, asistencia, intermediación, diseño e ingeniería corporativa, pago electrónico en línea de bienes que se envían por correo u otro servicio de mensajería, envío de servicios en línea como publicaciones, software, información, agencia de viajes, concesión de licencias, comisión, consignación, consultoría, distribución, intercambio, inversión, financiación, banca, empresa conjunta, cooperación industrial o comercial, factoraje (*factoring*); arrendamiento de bienes de equipo con opción de compra (*leasing*); seguros, suministro, transporte, contratos celebrados para la venta de bienes o prestación de servicios relacionados con medios electrónicos de información, etcétera.

El desarrollo tecnológico en la práctica mercantil internacional a partir de la década de los noventa, ha tenido la creciente tendencia en su uso; lo que, ha derivado

¹⁴ Joan Hortalà i Vallvé, Franco Roccatagliata y Piergiorgio Valente, *La fiscalidad del comercio electrónico*, Editorial CISS, Sociedad Anónima, Primera edición, Bilbao, 2000, p.p. 313.

en la creación de foros internacionales; ello, con el propósito de obtener certidumbre para generar obligaciones y vínculos jurídicos entre las partes; un ejemplo notable, es la Comisión de Naciones Unidas para el Derecho Mercantil Internacional –en inglés *United Nations Commission on International Trade Law* (UNCITRAL)-, de la Asamblea de las Naciones Unidas en 1996, que aprobó en cumplimiento de su mandato de fomentar la armonización y unificación del derecho mercantil internacional, la **Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico y otros medios conexos de comunicación de datos.**

Todo ello visualiza sin duda, nuevas oportunidades de crecimiento en las economías de aquellos que han decidido renovar sus procesos y romper con los moldes. La consolidación de un mercado abierto y ágil que estimule el crecimiento económico de una nación.

No es suficiente tener la intención, sino además, la participación activa de los gobiernos, empresas y consumidores, a favor de la edificación y consolidación de una economía creciente a través del uso y manejo de la tecnología.

Las perspectivas son buenas, sólo merece esfuerzo y ser valientes a los cambios que se presentan, en un ánimo innovador, de nuevas propuestas, y nuevas reflexiones, para alcanzar las metas y el desarrollo que conviene a nuestro país.

1.2 Tipos de comercio electrónico.

En el comercio electrónico participan como actores o agentes principales: “*empresas, consumidores y administraciones públicas.*”¹⁵

De las relaciones de estos tres actores, derivan tres tipos básicos de comercio electrónico; los que se conceptualizan como *negocios electrónicos*, a saber:

¹⁵ Téllez Valdés Julio, *Derecho Informático*, ob cit, pág. 218.

- Entre empresas o **B2B** (*Business to Business*)
- Entre empresa y consumidor o **B2C** (*Business to Consumers*)
- Entre empresa y la administración o **B2A** (*Business to Administration*)

B2B (*Business to Business*)

Esta modalidad engloba las transacciones realizadas entre empresas, esto es, en la que el cliente es un asociado o un proveedor; lo que, permite el fácil intercambio de bienes y servicios entre los concertantes a través de una *extranet*, considerada ésta, como una red privada de comunicación de las organizaciones que dan acceso no solo a sus miembros, sino a un grupo más grande de beneficiarios mediante la utilización de una clave de acceso; esto es, proveedores, socios comerciales y otros usuarios autorizados. El modelo de *e-business* aplicable a esta categoría cuenta con diversos elementos, como lo son: un centro de procesamiento de pedidos u órdenes de compra; accesos restringidos y accesos públicos; procesamiento de pagos y créditos; control de inventarios; historial de clientes y proveedores; catálogo de productos; y, logística de entrega.

B2B, es una modalidad a través de la cual se consolida la comunicación entre empresas y se desarrolla confianza por la seriedad y compromiso que transmiten; pues, a través de esta categoría de negocio, se maximiza el grado de satisfacción entre las empresas partes, y beneficia de forma adicional a los concertantes en la disminución de costos, y en la edificación de nuevas formas de hacer negocios.

B2C (*Business to Consumers*)

Refiere a la relación entre empresa y consumidor, la cual inicia a través de la investigación de mercado en línea, cuyo resultado advierte cuáles son las necesidades del comprador, para así, estar en aptitud de ofrecer los bienes y servicios que exactamente requiere.

Este modelo, con el establecimiento de *tienda virtual*, *tienda electrónica* o *e-shop*, genera ingresos a través de la venta de productos y servicios en línea. El *e-business* aplicado a esta modalidad conviene contar con las siguientes características en la página web: catálogo de productos; información adicional sobre los productos; precios; inventarios; tiempos y costos de entrega; formas de pago y líneas de crédito; ambiente de seguridad; canastas o carritos de compra; y, publicidad; no obstante, puede contar con otra característica adicional, lo cual incrementa el nivel de satisfacción del consumidor.

B2A (*Business to Administration*)

Bajo esta apertura comercial, se interrelacionan las personas y la administración pública, tal es el caso, de la información que ofrecen los gobiernos a través de sus páginas web, u organismos públicos, que ofrecen información al usuario.¹⁶

1.3 El derecho informático.

Derivado de la importancia de la *información*, la cual ha sido considerada como elemento fundamental para la toma de decisiones, y como lo afirma el escritor Miguel Ángel Davara Rodríguez, que “la información contribuye de una forma directa a la difusión de conocimientos, a la formación de las personas”,¹⁷ surge el derecho informático como regulador del tratamiento automatizado de la información, llamado *informática*; término formulado por el autor Phillippe Dreyfus, en el año de 1962.

1.3.1. Nociones básicas.

¹⁶ Cfr. Cavazos Arroyo Judith y Reyes Guerrero Soraya, *Comercio Electrónico: un enfoque de modelos de negocio*, op cit, p.p. 176-178.

¹⁷ Davara Rodríguez, Miguel Ángel, *Manual de Derecho Informático*, editorial Arazandi, Sociedad Anónima, Séptima edición, Navarra, 2005, p.p. 45.

Como exponente de esta nueva rama del conocimiento jurídico se menciona a *Norbert Wiener*, quien dedicado al derecho y a las comunicaciones, en 1949 con su obra “*Cibernética y sociedad*”, expresa la influencia que ejerce la cibernética respecto de uno de los fenómenos sociales más significativos: lo jurídico.

Por otro lado, cabe citar al juez estadounidense Lee Loevinger, quien publicó un artículo en la revista *Minnesota Law Review* titulado “*The Next Step Forward*”, en el cual manifiesta que, el próximo paso adelante en el largo camino del progreso del hombre, debe ser el de la transición de la teoría general del derecho hacia la jurimetría, que es la investigación científica acerca de los problemas jurídicos.

No obstante que en esa época no era predominante el avance tecnológico, se comienza a dilucidar el ánimo tanto de investigadores como de juzgadores, de estudiar las herramientas con las que han sido dotadas la información y las comunicaciones, dentro de un marco jurídico.

El ***derecho informático***, “es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica), y como objeto de estudio (derecho de la informática).”¹⁸

De allí, se desprenden dos conceptos; el primero, en sentido técnico, y el segundo, en sentido jurídico.

El derecho informático, en *sentido técnico*, es la práctica jurídica a través de la utilización de la tecnología; esto es, cuando las aplicaciones de la informática son utilizadas en la práctica del derecho (informática jurídica).

En *sentido jurídico*, el derecho informático es un sistema de normas que regulan las técnicas destinadas al tratamiento lógico y automatizado de la información, es decir, cuando el fenómeno de las tecnologías de la información y las comunicaciones son materia de estudio del derecho (derecho de la informática).

¹⁸ Téllez Valdés, Julio, *Derecho Informático*, ob cit, pág. 9.

1.3.2 Características fundamentales.

Fundamentalmente, se encuentran cinco características del derecho informático, a saber:

1. Nueva rama del conocimiento jurídico.
2. Disciplina que se encuentra en continuo desarrollo.
3. Constituida por dos vertientes: informática jurídica y derecho de la informática.
4. Se interrelaciona con otras ciencias y técnicas, tal es el caso de la cibernética (ciencia de la comunicación y control entre el hombre y la máquina), la informática, así como con su instrumento operativo, la computadora.
5. Alcanza los órdenes de carácter social, económico y político.¹⁹

Dichas características advierten la importancia de adquirir ciencia y conocimiento. El estudio de las distintas ramas en las que converge el derecho informático, es una premisa, para alcanzar la armonización del derecho con la tecnología. En su haber, el derecho informático conoce de la técnica, usos, legislación, desarrollo, control y gestión, regulación, propiedad intelectual, información, datos personales, gobierno, comunicación, contratos, comercio, aspectos laborales, prueba, delitos informáticos, derecho comparado, etcétera. Esto, crea una visión de desarrollo continuo, que merece ser estudiado y consolidado en cada nación y gobierno.

1.3.3 Informática jurídica.

La informática jurídica es el conjunto de aplicaciones de la informática en el

¹⁹ Cfr. *Ibidem*, p.p. 8.

ámbito del derecho.

Nace propiamente en 1959 en Estados Unidos, derivado de los esfuerzos realizados en el Health Law Center (HCL) de la Universidad de Pittsburgh, Pensilvania, cuyo director John Horty, convencido de la necesidad de encontrar medios idóneos para tener acceso a la información legal, se colocaron los ordenamientos legales de Pensilvania en cintas magnéticas.

Explicado este sistema en 1960 ante la American Bar Association (ABA) (Asociación Americana de la Barra de Abogados), en la reunión anual celebrada en Washington, D.C; era la primer demostración de un sistema legal automatizado de búsqueda de información.

El autor Julio Téllez Valdés, define la informática jurídica como: “la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como a la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación”.²⁰

Esta técnica interdisciplinaria ha tenido etapas o incursiones, en las cuales ha evolucionado la utilización de las ventajas que representa la recuperación de información jurídica, a través de los sistemas, a saber:

1. El sistema Health Law Center (HLC), por medio del cual la Corporación Americana de Recuperación de Datos, en 1964, comenzó a comercializar sistemas de procesamiento de datos legislativos.
2. El sistema OBAR, enfocado hacia los litigantes, comenzó en 1967, cuando la Corporación de Investigación Automatizada de la Barra de Ohio firmó un contrato con la Corporación de Datos

²⁰ Téllez Valdés, Julio, *Derecho Informático*, ob cit, pág. 10.

de Dayton, Ohio. En 1970, luego de la fusión de Data Corporation con Mead Corporation, la Mead Data Central (CMD), continuó los trabajos de este sistema.

3. El sistema LEXIS, como sucesor del OBAR, en 1973, la Mead Data Central lo comenzó a comercializar. Actualmente es el sistema de informática jurídica mas importante y rentable a nivel mundial.²¹

El desarrollo de está técnica llamada informática jurídica, ha dado origen desde su inicio a la informática jurídica *documentaria, metadocumentaria y de gestión*; los cuales se exponen en lo conducente, a continuación:

Informática jurídica documentaria.

Es el área más antigua de la informática jurídica. En los sistemas de informática jurídica documentaria se trata de crear un banco de datos jurídicos o *corpus* jurídico documentario, relativo a cualquiera de las fuentes del derecho, excepto la costumbre; cuyo rendimiento está en función de la exactitud y extensión de los datos contenidos y de los criterios de búsqueda de los documentos (leyes, acuerdos, reglamentos doctrina, jurisprudencia). Los *batch*, fueron los primeros sistemas de interrogación de bancos de datos jurídicos, que permitían la búsqueda en los archivos, esto es, de textos y de palabras ordenadas alfabéticamente, que indicaban, una vez señalada una palabra, la “dirección” donde estaba almacenada..

El propósito de la informática en un sistema documentario, consistente en encontrar de manera rápida la información que ha sido almacenada en el banco de datos o *corpus*, el cual, constituye el conjunto de esas informaciones, que son contenidas a través de la interfase almacenamiento-recuperación de información jurídica, cuyo proceso inicia con la entrada de documentos, bajo una forma codificada

²¹ Cfr. *Ibidem*, p.p. 11.

comprensible para la máquina, y cuya codificación de textos será más o menos voluminosa según la capacidad del sistema.

Algunos de los sistemas en operación a nivel informática jurídica documentaria, se encuentran: Lexis.nexis; italgire find (de la Suprema Corte de Casación de Italia); IDG (del Instituto para la Documentación Jurídica de Florencia, Italia); Celex (de la Comunidad Europea con sede en Bruselas); Prodasen (de la Cámara de Senadores, Brasil); Credoc (de la Federación Real de Abogados y Notarios, Bélgica, el más antiguo en Europa); en México, se encuentran, UNAM-IURE (del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México), IUS (de la Suprema Corte de Justicia de la Nación), el de la Cámara de Diputados, el de la Cámara de Senadores, el de Orden Jurídico Nacional de la Secretaría de Gobernación, Lexis-México, y V/Lex.²²

Informática jurídica metadocumentaria.

Es un tipo de aplicación de la informática que va más allá de un banco de datos jurídicos, pues incorpora la asistencia máxima al usuario en sus distintas vertientes: *decisional*, *educativa*, *investigación*, *previsión* y *redacción*.

La asistencia *decisional*, a través de “sistemas expertos”, que es un sistema informático que se utiliza como instrumento para resolver problemas, mediante el uso de razonamientos implementados en la computadora. Dicho sistema, contiene una base de conocimientos en forma de banco de datos bien estructurado; un sistema cognoscitivo o mecanismo de inferencia que contiene la mayor parte de los esquemas y razonamiento válidos en ese dominio; y, una interfase que comunica al usuario con la máquina.

La asistencia en el plano de la *educación*, se consolida a través de la aplicación de las nuevas tecnologías de información y comunicación (TIC), en la enseñanza del derecho; toda vez que, genera un nuevo sistema de aprendizaje del

²² Cfr. Téllez Valdés, Julio, *Derecho Informático*, ob. cit, p.p. 17-24.

derecho en una sociedad informatizada, que consolida al jurista en su profesión, y al estudiante en su formación jurídico-educacional.

La asistencia en *investigación*, llamada informática jurídica de investigación o informática jurídica analítica, desarrolla el descubrimiento de aquellos instrumentos matemáticos que puedan revestir utilidad, en esa tesitura, utiliza las mayores capacidades de la máquina para poner a prueba las hipótesis y teorías jurídicas, llamado así “repensar del derecho”.

La asistencia a la *previsión*, basada en el análisis de bancos de datos multidimensionales correspondientes a una serie de objetos o individuos que facilita la computadora; de tal manera, que se puede derivar el orden de prioridad de factores explicativos de esos datos; de ello toma su nombre de análisis factorial, dado el conjunto de esos métodos de examen. Este análisis ha permitido desarrollar extensamente los trabajos experimentales basados en la interpretación de observaciones múltiples. Las decisiones jurisdiccionales y la jurisprudencia, entre otras, derivan en soluciones jurídicas, que a la postre, un asunto que tenga la serie de factores de los cuales derivaron dichas resoluciones y criterios, podrá “predecir” el desenlace del caso.

Si es el caso de decisiones contradictorias, el análisis factorial podrá, bajo reserva de variadas condiciones, convertirse en un instrumento importante para prever la clasificación del nuevo caso sometido. La previsión o predicción de las decisiones judiciales es por antonomasia el dominio de elección de los métodos de análisis de datos jurídicos, particularmente en los países anglosajones, donde han desarrollado sus técnicas a causa de la referencia sistemática al precedente (*stare decisis*).

La asistencia a la *redacción*, consisten en programas que corrigen de fondo para ajustar el texto a las intenciones legislativas y todas las modificaciones de forma que faciliten la comprensión del texto. Provee un apoyo informático permanente al momento de la concepción del texto de la ley. Esto es, las diferentes proposiciones del texto en vía de elaboración aparecen en la pantalla acorde con una búsqueda, no

simplemente en función de un texto seguido, sino según una estructuración que corresponde a la lógica interna del texto.²³

Informática jurídica de control y gestión.

El aspecto documentario no es el único que se ha desarrollado dentro de la informática jurídica, pues otras áreas desde hace tiempo se desarrollan, como lo es la llamada *informática jurídica de control y gestión*, cuyo antecedente se remonta el tratamiento de textos jurídicos mediante el uso de procesadoras de palabra, así como las experiencias emanadas en materia de automatización de registros públicos. Esta rama alcanza fundamentalmente los ámbitos jurídico-administrativo, judicial, registral y despachos de abogados.

La utilización de esta herramienta en la administración pública ha presentado avances en la operación de las distintas actividades en las dependencias gubernamentales; asimismo, agiliza la tramitación de asuntos jurídico administrativos, lo que ha obligado a los diferentes niveles de gobierno, capacitarse para efecto de recibir, tramitar, analizar y difundir todo tipo de información jurídica para su correcto funcionamiento, lo que ha evolucionado las estructuras y los sistemas de operación.

La aplicación de la informática en las actividades de los órganos jurisdiccionales, ha dado origen a la *informática judicial*. Ello, incorpora nuevos conocimientos e innovaciones, que dilucidan un alcance cada vez mayor de la informática en la actividad jurisdiccional, y por ende, una mayor injerencia de los magistrados y jueces, para allegarse de los medios electrónicos que asistan a una impartición de justicia pronta, completa e imparcial. Ejemplos notables, el seguimiento de expedientes, el expediente electrónico, el sistema computarizado para el registro único de profesionales del derecho, denuncias por Internet, pago de impuestos por Internet, el sistema de registro de inscripción automática de demandas para su remisión al órgano jurisdiccional en turno, consulta de tesis jurisprudenciales

²³ Cfr. *Ibidem*, p.p. 26-33.

vía electrónica, consulta vía telemática de los asuntos tratados ante un tribunal (ciberjusticia o cibertribunales).

De igual manera, el uso de la informática en notarias y despachos, constituye una herramienta que automatiza las actividades de la oficina. En el campo notarial, ofrece organización, control y alcance, de la agenda, estados de asuntos, registros, tarifas, cálculos de impuestos y demás acciones de carácter notarial. De igual manera, la automatización de las oficinas con actividades jurídicas, o llamada, *ofimática jurídica*, ha simplificado las labores propias de los despachos de abogados, mediante el uso de sistemas automatizados como control de asuntos con horarios, redacción de escritos, actualización de criterios jurisprudenciales, doctrina, bibliografía, etcétera.²⁴

1.3.4 Derecho de la informática.

El derecho de la informática, es el sistema de normas que regulan a la informática, entendida ésta como la ciencia del tratamiento automatizado de la información.

Es “el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática”.²⁵

En atención a la forma de tratamiento de la información y su regulación, el derecho de la informática se ha dividido en: *política informática* y *legislación informática*.

La ***política informática***, trata con el adecuado desarrollo de la industria de construcción de equipos de cómputo y de programación, planeación, difusión y aplicación del fenómeno informático, la contratación gubernamental de bienes y servicios informáticos; la formulación de normas y estándares en materia informática, así como el control de importaciones y exportaciones sobre equipos accesorios y

²⁴ Cfr. *Ibidem*, p.p. 24-26.

²⁵ Téllez Valdés, Julio, *Derecho Informático*, ob cit, pág. 13.

programas de computadoras.

Por otro lado, la **legislación informática**, es un sistema de normas que emanan del uso de la informática que regulan diversas áreas, entre otras, a saber: *protección de la información y de los datos personales; regulación jurídica del flujo internacional de datos; regulación jurídica de Internet; propiedad intelectual y las nuevas tecnologías de la información y comunicación; contratos informáticos; spam; aspectos laborales de la informática; documentos electrónicos o informáticos y su valor probatorio*; las cuales en lo conducente se exponen a continuación:²⁶

Protección de la información y de los datos personales.

El derecho informático, en su vertiente de derecho de la informática, regula y protege la información y los datos personales que han sido objeto de tratamiento automatizado. Ejemplo notable, el artículo 6° y 16, de nuestra Constitución Política, que expresan respectivamente, la tutela que tiene el Estado sobre la información y los datos personales; así como la facultad que tiene el Congreso para legislar en materia de protección de datos personales en posesión de particulares, regulado en el 73, numeral XXI-O, de la propia Carta Magna; dispositivos que fueron punta de lanza para que años subsecuentes el Congreso de los Estados Unidos Mexicanos, decretara la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Regulación jurídica del flujo internacional de datos.

Es la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y recuperación. Como beneficios se encuentra que representa un aliado del derecho a la información, y una herramienta que consolida la confianza entre los países, el desarrollo de nuevos conocimientos, así como la cooperación económica entre los países; como detrimento de este flujo de información, se ha considerado que vulnera, en alguna parte, la integridad de la

²⁶ Cfr. *Ibidem*, pág. 12.

nación, en el caso de que información salga del país (soberanía nacional), o bien, en el caso de que dicha información entre al país, que pueda amenazar su identidad cultural (transculturación).

Existen diferentes flujos de información: *comercial* (servicios documentarios, base de datos, comercialización); *empresarial* (dirección, decisión, administración y operación de las empresas); y, *especial* (actividades educativas y de investigación).

Dichas informaciones circulan por redes, según el tipo de datos que fluyen, entre otras, a saber: SITA (Red de la Sociedad Internacional de Telecomunicaciones Aeronáuticas); SWIFT –siglas en ingles- (Red Bancaria de Intercambio de Mensajes Financieros); NICS –siglas en ingles- (Red de la Policía Internacional); INTERNET (*Interconnected networks*).

Es así como diversos organismos gubernamentales y no gubernamentales se han ocupado en conformar un marco regulatorio sobre este fenómeno internacional, entre los que destacan: la Organización para la Cooperación del Desarrollo Económico (OCDE); Centro de Corporaciones Transnacionales de las Naciones Unidas (UNCTC); la Organización Mundial de Comercio (OMC); la Comisión de Comercio y Desarrollo de las Naciones Unidas (UNCTAD); la Organización Mundial de la Propiedad Intelectual (OMPI); la Corporación de Internet para la Asignación de Nombres y Números (en ingles: Internet Corporation for Assigned Names and Numbers; ICANN); y, la Unión Europea (UE).²⁷

Regulación jurídica de Internet.

Internet, es una infraestructura constituida por protocolos que permite el enlace de computadoras por todo el mundo, la cual, no obstante se concibió como un sistema descentralizado, y aparentemente bajo sin ninguna autoridad o gobierno central que lo regule, lo cierto es que las conductas llevadas a cabo con ayuda de esta

²⁷ Cfr. Ibidem, p.p. 93-107.

red no están exentas del cumplimiento de la norma jurídica; ello, en virtud de que se encuentra sometida a una jurisdicción, competencia, y legislación aplicable.

En cuanto a la jurisdicción, se ha considerado que el Estado al que corresponde tener conocimiento de las controversias que se susciten en esta materia, será el del lugar donde fue emitida la comunicación o materializada, esto es, en atención al lugar de emisión o de recepción.²⁸

Por lo que hace a la competencia, corresponde a los jueces federales, conocer de los asuntos relacionados con Internet, en sus distintas materias, sea el caso.

Respecto de la legislación aplicable, se han establecido diversos principios, a saber: la *libre escogencia de la ley aplicable al contrato electrónico*, que es un acuerdo entre las partes sobre la elección del derecho aplicable; *tratos o convenios internacionales*, en el caso de que no exista legislación aplicable elegida por las partes contractuales; “*autonomía de la voluntad*”, que genera una autorregulación sin sometimiento a normativa estatal, salvo en las normas de protección de los consumidores y usuarios; y, el *derecho uniforme transaccional*, que vela por armonizar las políticas y unificar criterios entre las naciones, como ejemplo, se encuentran diversas organizaciones, entre otras, OMPI-WIPO, la OMC-WTO, UNCITRAL-CNUDMI).²⁹

Propiedad intelectual y las nuevas tecnologías de la información y comunicación.

Se destaca en este apartado la protección jurídica de los programas de computación (software), métodos de negocios, y la de los llamados, nombres dominio.

²⁸ Cfr. Universidad de los Andes, Facultad de Derecho, Internet, *Comercio Electrónico & Telecomunicaciones*, ob cit, p.p. 478 y 479.

²⁹ Cfr. Ibidem, págs. 489-490.

Estados Unidos, país pionero en esta materia, luego de que derivado de las decisiones jurisdiccionales, excluía como patentable al *software* por considerarlas como ideas abstractas, y a los *métodos de negocios*, de quienes argumentaba que le faltaba el elemento tecnológico; actualmente se reconoce la protección de ambos con tal carácter. Ello, ha favorecido el desarrollo de las industrias relacionadas en éste ámbito en dicha nación.

Por su parte, al seno de la Unión Europea, la Dirección General para el Mercado Interno de la Comisión Europea, ha publicado su propuesta de directiva europea, en el sentido de exponer la admisión de las patentes relacionadas con programas informáticos, e invitar a los países miembros a armonizar las legislaciones sobre patentes de inventos que requieran un programa informático, con la salvedad de que la invención debe aportar una contribución técnica.

En Japón, se ha interpretado en el mismo sentido que la Unión Europea; a favor de que la invención sea una creación muy avanzada de conceptos técnicos mediante la cual se aplique una ley natural.

A diferencia de las anteriores, la Organización Mundial de la Propiedad Intelectual, integra a los programas informáticos dentro del derecho de autor, mismos que gozan de protección con arreglo con esta normativa varios países, y en atención al Tratado de la OMPI sobre el Derecho del Autor, no obstante esta categoría no figure en la lista del Convenio de Berna.

De la misma manera, en nuestro país se reconoce a los programas de cómputo dentro de los derechos de autor; de conformidad con el artículo 13 de la Ley Federal del Derecho de Autor; no así a los modelos de negocios, en atención al artículo 14, fracción III, de la dicho ordenamiento.

Bajo esos criterios, considero que el software es una invención, en virtud de que es susceptible de aplicación industrial, además de que puede promover una solución técnica a un problema; no obstante, que puede tratarse a través de la

normativa de los derechos de autor como una obra científica, esto es, en su carácter de producciones en el área científica.

Por cuanto hace al *nombre de dominio*, definido este como: “el nombre asociado a un sitio o lugar en la red.”³⁰; esto es, “un medio de identificación y ubicación en el Internet”,³¹ ICANN (Internet Corporation for Assigned Names and Numbers) es la encargada del control de su sistema, y junto con la OMPI, han aprobado paneles para resolver conflictos que se susciten en esta materia.

En México, el Registro de Nombres de Dominio (CCTLD.MX), es administrado por el Centro de Servicios de Información y Registro en Internet, NIC-México, del Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Monterrey por delegación de IANA e ICANN, bajo los principios del documento RFC-1591.

Contratos informáticos.

El artículo 1794, del Código Civil Federal, señala que para la existencia del contrato se requiere de los siguientes elementos: I. Consentimiento; y, II. Objeto que pueda ser materia del contrato; llamados éstos elementos de existencia, ó como los conceptúa el autor Rafael Rojina Villegas, en “elementos esenciales”.³²

Asimismo, los elementos de validez, son: I. Capacidad legal de las partes o de una de ellas; II. Ausencia de vicios del consentimiento; III. Objeto, o su motivo o fin sea lícito; y, IV. Consentimiento se haya manifestado en la forma que la ley establece. Elementos que se desprenden del artículo 1795, del citado ordenamiento, en sentido contrario.

“La diferenciación de los elementos de existencia de los de validez es un progreso de técnica jurídica que permite explicar y sistematizar las diversas

³⁰ Davara Rodríguez, Miguel Ángel, *Manual de Derecho Informático*, editorial Arazandi, Sociedad Anónima, Séptima edición, Navarra, 2005, pág. 218.

³¹ Universidad de los Andes, Facultad de Derecho, Internet, *Comercio Electrónico & Telecomunicaciones*, ob cit, pág. 354.

³² Rojina Villegas, Rafael, *Teoría General de las Obligaciones*, Tomo III, editorial Porrúa, Sociedad Anónima de Capital Variable, Vigésimo Séptima edición, México, 2007, pág. 54.

consecuencias producidas por la ausencia de alguno de ellos. Si falta un elemento esencial, el acto no existe como tal. Si está ausente un requisito de validez el acto existe, pero puede ser invalidado”.³³

En esa tesitura, el contrato informático, es el convenio que produce o transfiere las obligaciones y derechos sobre bienes o servicios informáticos. Como cualquier contrato, el contrato informático para que sea existente y válido, debe reunir los elementos que citan tales numerales.

El autor peruano Willheim David Angermüller, define contrato informático, como: “el acuerdo de voluntades de dos o más partes con el fin de crear vínculos de obligaciones y que busca crear, regular, modificar o extinguir una relación jurídica patrimonial, cuya prestación debe estar relacionada en todo o en parte con el proceso informático: un hardware, un software, un servicio informático, datos ofrecidos por las computadoras o servicios informáticos múltiples o complejos.”³⁴

El escritor Emilio del Peso, define al contrato informático como “aquel cuyo objeto sea un bien o servicio informático –o ambos- o en el que una de las prestaciones de las partes tenga por objeto ese bien o servicio informático”.³⁵

Los *bienes informáticos*, son “todos aquellos elementos que forman el sistema –ordenador- en cuanto al hardware, ya sea la unidad central de proceso o sus periféricos, y todos los equipos que tiene una relación directa de uso con respecto a ellos y que, en su conjunto, conforman el soporte físico del elemento informático, así como los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático.”³⁶

³³ Bejarano Sánchez, Manuel, *Obligaciones Civiles*, Oxford University Press México, Sociedad Anónima de Capital Variable, Quinta edición, México 1999, pág. 41.

³⁴ Téllez Valdés, Julio, *Derecho Informático*, ob. cit, pág. 142.

³⁵ Téllez Valdés, Julio, *Derecho Informático*, ob. cit, pág. 143.

³⁶ *Ibidem*, p.p. 135.

Asimismo, los *servicios informáticos*, son “todos aquellos que sirven de apoyo y complemento a la actividad informática en una relación de afinidad directa con ella”.³⁷

Se han clasificado los contratos informáticos, por su *objeto y negocio jurídico*.

Por cuanto hace a su **objeto**, los contratos informáticos se clasifican en: contratos de hardware; contratos de software; contratos de instalación llave en mano; y, contratos de servicios auxiliares.³⁸

Los contratos informáticos, por lo que refiere al **negocio jurídico**, se clasifican en: compraventa; arrendamiento; arrendamiento financiero o leasing; de mantenimiento; de prestación de servicios; de arrendamiento de obra; de préstamo; y, de depósito.³⁹

En cuanto a la **relación contractual**, se ha considerado la naturaleza jurídica del contrato informático, caracterizándolo de acuerdo a la clasificación de los contratos, como un contrato: bilateral, conmutativo, formal-atípico, complejo, híbrido, de adhesión, principal, oneroso, instantáneo y de tracto sucesivo, consensual, y *sui generis*.⁴⁰

Finalmente, cabe mencionar al seguro informático, en cuya póliza se busca que cubra todos y cada uno de los riesgos informáticos, definido éstos como aquellos eventos circunstanciales que provocan un daño a los bienes o servicios informáticos; y, en ese sentido, no se adopten las pólizas convencionales.⁴¹

Contrato electrónico o contratación electrónica.

³⁷ Ibidem, p.p. 136.

³⁸ Cfr. Ibidem, p.p. 152.

³⁹ Cfr. Davara Rodríguez, Miguel Ángel, ob. cit, pág. 218.

⁴⁰ Cfr. Téllez Valdés, Julio, ob. cit. Pág. 142.

⁴¹ Ibidem, p.p. 158.

También llamada contratación con asistencia informática, o contratación por medios electrónicos o informáticos.

A diferencia del contrato informático, el contrato electrónico es un contrato celebrado mediante dispositivos automáticos, principalmente por Internet; ya sea de forma directa o indirecta.

Un contrato electrónico se realiza de forma *directa*, cuando las personas directamente ejecutan las ordenes a través de la computadora.

Es *indirecta*, cuando las órdenes son ejecutadas automáticamente por los medios electrónicos; sin embargo, esta forma representa problemas en los costos, infraestructura y operación; un ejemplo, es el sistema de Electronic Data Interchange (EDI), el cual, es un sistema que estandariza procesos de negociación entre compañías, que permite localizar y revisar los procesos de documentos comunes, como órdenes de compra, facturas, manifiestos de aduana, calendarios de envíos, y otros documentos derivados de la actividad comercial de las compañías.

Los contratos electrónicos se perfeccionan por el mero consentimiento expreso, al momento en que el proponente reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada; entendido el consentimiento, como “un acuerdo de voluntades”,⁴² cuyos elementos que lo integran “son las dos manifestaciones de voluntad llamadas Oferta y Aceptación”.⁴³

Ello, lo señalan los numerales 80 del Código de Comercio; así como a los artículos 1803 y 1807, del Código Civil Federal; que a la letra indican, respectivamente:

“Artículo 80. Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de

⁴² Martínez Alfaro, Joaquín, *Teoría de las obligaciones*, editorial Porrúa, Sociedad Anónima de Capital Variable, Décimo Primera edición, México, 2008, pág. 56.

⁴³ Ídem.

cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.”.

“**Artículo 1803.** El consentimiento puede ser **expreso** o tácito, para ello se estará a lo siguiente:- - - I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por **medios electrónicos**, ópticos o por cualquier otra tecnología, o por signos inequívocos.” (resalto)

“**Artículo 1807.** El contrato se forma en el momento en que el proponente reciba la aceptación, estando ligado por su oferta según los artículos precedentes.”

Dichos dispositivos legales son concordantes con el sistema propuesto en la Ley Modelo sobre Comercio Electrónico de las Naciones Unidas, llamado, “confirmación de recepción”; entendida ésta, como la confirmación de la aceptación de la oferta.

Spam.

La palabra *spam*, surge de la contratación de los productos de comida enlatada llamada *Shoulder Pork and hAM/SPiced hAM* (spam), que era enviada de forma masiva a las tropas estadounidenses durante la Segunda Guerra Mundial. De ahí deriva el concepto Spam, para referirse a la práctica de enviar correo de manera indiscriminada a través de la red de Internet, sin importar el receptor final del correo, esto es, un modo masivo de publicitar productos o servicios.

Hace aproximadamente once años, una pareja de abogados en Nueva York, que buscaban promocionar su despacho a un número grande de clientes con el menor costo posible, sin tener listas de usuarios de correos electrónicos, usaron las direcciones de sus clientes de manera que ellos lo reenviaran a sus conocidos, convirtiéndose en un mercado directo y en spam.

El Proyecto Norteamericano sobre Protección al Consumidor en Comercio Electrónico (North American Consumer Project on Electronic Commerce –sus siglas

en inglés, NACPEC-), define al spam, como el correo comercial no solicitado, generalmente enviado a las direcciones electrónicas de los consumidores sin su autorización y consentimiento.

Existe también el *Scam* u *Junk mail* (correo chatarra), utilizado para referirse a correos relacionados con publicidad engañosa (pornografía), y cadenas (correos que incluyen textos en los que se solicitan sean reenviados a otras personas). El *Spim*, utilizado por medio de la mensajería instantánea; *phishing*, cuyo objetivo es por medio de sitios que se asemejan a los de los bancos, sistemas de pago o proveedores, arguyendo una falla en el sistema o que la información no se ha actualizado debidamente, y solicitando al consumidor acceder a una página web por medio de un *link* o enlace, para obtener información de carácter personal, como datos personales, números de cuenta de tarjetas de crédito o tarjetas de débito, passwords o NIP (número de i), dirección, teléfono, etcétera.

Ante ello, se han adoptado medidas legales en distintos países con el propósito de limitar y regular esta práctica. En México, el spam se encuentra regulado por la Ley Federal de Protección al Consumidor, en sus artículos 17, 18, 76 bis y 128.

El reto en esta área es que conforme al avance de la tecnología, se adecuen los programas de acción, y se pueda tener transparencia de los mensajes que se reciban, para así evitar que cualquier información no idónea llegue a los correos electrónicos.

44

Aspectos laborales de la informática: ergonomía y teletrabajo.

Son las relaciones obrero-patronales en las cuáles interviene la informática.

Ergonomía informática, proviene de *ergon*, que significa energía, trabajo; *nomos*, que significa *tratado*; y, del vocablo *informática*, que es el conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información. Esto es, la

⁴⁴ Cfr. Téllez Valdés, Julio, *ob cit*, págs. 253-262.

ergonomía es el conjunto de implicaciones de orden normativo-laboral provocadas por el uso de la informática; ejemplo de ello, la movilización de puestos (desplazamiento laboral), y las condiciones de trabajo (jornada de trabajo, vacaciones, salario).⁴⁵

El **teletrabajo**, es la “forma flexible de organización del trabajo, que consiste en el desempeño de la actividad profesional sin la presencia física del trabajador de la empresa durante una parte importante de su horario laboral.”⁴⁶

Es “una forma flexible de organización del trabajo que se realiza con ayuda de las tecnologías de la información y las comunicaciones, en un lugar distinto y alejado del que ocupa la organización o la persona para quien se realiza el trabajo.”⁴⁷

Se destacan cuatro puntos de esta nueva forma de relación laboral:

- 1) El trabajo se lleva a cabo fuera del entorno usual de la oficina, esto es, se lleva a cabo en centros de trabajo cercanos a las residencias de los teletrabajadores (*satellite office*).
- 2) Uso intensivo de las tecnologías de información.
- 3) Sistema de control de gestión altamente formalizado.
- 4) Sistemas de trabajo basados en la dirección por objetivos o en el trabajo por proyectos.⁴⁸

Asimismo, como ventajas del teletrabajo, se distinguen las siguientes: mejoras tecnológicas; avances en las telecomunicaciones; globalización de la economía; dinamismo de la empresa; *outsourcing* (cesión de la gestión de los sistemas de información de una entidad a un tercero); flexibilidad del horario para los trabajadores; reducción de costos en inmobiliario; sistema de control por objetivos-resultados; incremento de la productividad; alcance internacional de la empresa;

⁴⁵ Cfr. Téllez Valdés, Julio, ob. cit. pág. 263.

⁴⁶ Ibidem, p.p. 268 y 269.

⁴⁷ Ibidem, p.p. 269.

⁴⁸ Cfr. Ibidem, p.p. 269.

fortalecimiento de mercado; mejora en la calidad del trabajo; permanencia del servicio; reducción de los desplazamientos del trabajador; y, reducción de tránsito vehicular.⁴⁹

De la misma forma, se dilucidan como desventajas, entre otros: falta de interacción diaria entre compañeros; individualismo; costos de los equipos e infraestructura; estancamiento profesional; distracciones del trabajador; división de intereses; contratos por horas de trabajo; el trabajo al realizarse en casa puede imperar directamente en requerimientos en el horario laboral de la familia al teletrabajador;⁵⁰ esto se puede concluir con lo siguiente: “Todo tiene un tiempo”.

Actualmente, la situación internacional no es uniforme en cuanto a la regulación del trabajo a domicilio. En nuestra nación, si bien no se encuentra regulado el teletrabajo como tal; sí se regula en la Ley Federal del Trabajo, en su capítulo XII, de los artículos 311 a 330, el “Trabajo a domicilio”, donde se define éste, como “el que se ejecuta habitualmente para un patrón, en el domicilio del trabajador o en un local libremente elegido por él, sin vigilancia ni dirección inmediata de quien proporciona el trabajo”.

De tal manera, que se puede concluir que el teletrabajo es una forma de trabajo a domicilio; en esa tesitura, solo queda adicionar las condiciones de esta nueva modalidad laboral en el citado ordenamiento legal.

Documentos electrónicos o informáticos y su valor probatorio.

El documento electrónico o mensaje de datos, es aquella información que se enseña o expresa, a través de un medio electrónico.

⁴⁹ Cfr. Téllez Valdés, Julio, págs. 272 y 273.

⁵⁰ Cfr. *Ibidem*, págs. 274-276.

Técnicamente, el documento electrónico, es “un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que, sometidos a un adecuado proceso, permiten su traducción a lenguaje natural mediante una pantalla o una impresora”.⁵¹

Asimismo, se define al documento electrónico, como “el formado por la computadora o dispositivo electrónico, a través de sus propios órganos de salida, y que es perceptible por el hombre sin la necesidad de máquinas traductoras.”⁵²

El autor Nelson Remolina Angarita, define el documento electrónico, como “aquellos documentos cuyo soporte se encuentra en medios electrónicos, llámese mensajes de datos, registro contable electrónico o el texto electrónico de un contrato.”⁵³

La escritora María Fernanda Guerrero, por su parte, afirma que el documento electrónico es “cualquier representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser asimilados en forma humanamente comprensible.”⁵⁴

A su vez, se han clasificado los documentos electrónicos en: documentos informáticos sobre soporte electrónico, y documentos informáticos sobre soporte papel.⁵⁵

Los **documentos informáticos sobre soporte electrónico**, son documentos producidos en la computadora, que pueden ser leídos con la aplicación de la técnica informática. Sólo tiene un soporte electrónico o soporte informático; asimismo, los **documentos informáticos sobre soporte de papel**, son documentos producidos por medio de la computadora, creados mediante el uso de un periférico de salida (impresora), y se le dota de soporte papel para ser leído.

⁵¹ Téllez Valdés, Julio, ob cit, pág. 292.

⁵² Ibídem, p.p. 293.

⁵³ Universidad de los Andes, Facultad de Derecho, Internet, ob cit, pág. 18.

⁵⁴ Ídem.

⁵⁵ Téllez Valdés, Julio, ob cit, pág. 297.

En la parte que interesa, en cuanto al **valor probatorio** de los mensajes de datos, el Código de Comercio, en sus artículos 1205 y 1298-A, establece lo siguiente:

“**Artículo 1205.** Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, **mensajes de datos**, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.”. (resalto)

“**Artículo 1298-A.** Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.”.

Asimismo, los artículos 188 y 210-A, del Código Federal de Procedimientos Civiles, refieren lo que a continuación se transcribe a continuación, respectivamente:

“**Artículo 188.** Para acreditar hechos o circunstancias en relación con el negocio que se ventila, pueden las partes presentar fotografías, escritos o notas taquigráficas, y, en general, toda clase de elementos aportados por los descubrimientos de la ciencia.”

“**Artículo 210-A.** Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.- - **Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.- -** Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará

satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.”(resalto)

De la lectura de dichos dispositivos, se advierte que estos son concordantes con la Ley Modelo de la CNUDMI sobre Comercio Electrónico, cuyo artículo 9º, establece que toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria; al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Derivado de dicha regulación, acorde a los principios establecidos por la Ley Modelo de la CNUDMI sobre Comercio Electrónico, han surgido diversos criterios relativos al valor probatorio de los mensajes de datos en diversas materias, entre éstos, existe jurisprudencia, entendida ésta como el “conjunto de principios y doctrinas contenidas en las decisiones de los tribunales”,⁵⁶ a saber:

- **Localización:** Novena Epoca, Instancia: Tribunales Colegiados de Circuito, Fuente: Semanario Judicial de la Federación y su Gaceta, XXX, Julio de 2009, Página: 1943, Tesis: I.7o.C.56 K, Tesis Aislada, Materia(s): Común.

“INTERNET. ES UNA MEDIDA PERTINENTE PARA INVESTIGAR EL DOMICILIO DE LA TERCERA PERJUDICADA SI SE TRATA DE UNA EMPRESA CUYOS DATOS SE LOCALICEN POR ESE MEDIO. Según la fracción II del artículo 30 de la Ley de Amparo, si no consta en autos el domicilio del tercero perjudicado, la autoridad que conozca del amparo dictará las medidas que estime pertinentes para investigar su domicilio. En la actualidad, un número creciente de empresas utiliza medios electrónicos para ofrecer sus productos y en ocasiones incluyen sus domicilios. Por su parte, el artículo 210-A del Código Federal de Procedimientos Civiles,

⁵⁶ García Maynez, Eduardo, *Introducción al Estudio del Derecho*, editorial Porrúa, Sociedad Anónima de Capital Variable, Quincuagésimo Primera edición, México, 2000, pág. 68.

de aplicación supletoria a la Ley de Amparo, reconoce como prueba la información generada o comunicada a través de medios electrónicos; y, tanto constitucional como jurisprudencialmente, el llamamiento a juicio se reconoce como una formalidad esencial del procedimiento de estudio oficioso y donde opera la suplencia de la queja. Por lo tanto, una de las medidas pertinentes que puede dictar la autoridad federal para localizar el domicilio de la parte tercera perjudicada, si se trata de una empresa cuya localización no conste en autos, es la de efectuar su búsqueda por internet a través de las diversas páginas que ofrecen dicho servicio, donde basta introducir el nombre de la empresa que se pretende localizar y en breve se despliega información de la que puede obtenerse la forma para contactar con dichas empresas y en algunos casos también proporcionan sus domicilios.”,

- **Localización:** Novena Epoca, Instancia: Tribunales Colegiados de Circuito, Fuente: Semanario Judicial de la Federación y su Gaceta, XXVI, Septiembre de 2007, Página: 2528, Tesis: I.4o.A.596 A, Tesis Aislada, Materia(s): Administrativa.

“ESTADOS DE CUENTA INDIVIDUALES DE LOS TRABAJADORES AFILIADOS AL INSTITUTO MEXICANO DEL SEGURO SOCIAL. PARA DETERMINAR SU VALOR PROBATORIO DEBEN EVALUARSE, ENTRE OTROS ASPECTOS, LOS REQUISITOS A QUE SE REFIERE EL SEGUNDO PÁRRAFO DEL ARTÍCULO 210-A DEL CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES, APLICADO SUPLETORIAMENTE, EN CUANTO A LA INFORMACIÓN GENERADA QUE CONSTE EN MEDIOS ELECTRÓNICOS, ÓPTICOS O EN CUALQUIER OTRA TECNOLOGÍA. De los artículos 3, 4, 5 y 14 del Reglamento del Seguro Social en Materia de Afiliación, Clasificación de Empresas, Recaudación y Fiscalización se advierte, por una parte, que el patrón debe inscribir a sus trabajadores en el Instituto Mexicano del Seguro Social y comunicarle sus modificaciones salariales y bajas, ya sea presentando los formatos impresos autorizados, o bien, a través de medios magnéticos, digitales, electrónicos, ópticos, magneto ópticos o de cualquier otra naturaleza, debiendo utilizar, en este caso, el número patronal de identificación electrónica que le proporciona el citado instituto, como llave pública de sus sistemas criptográficos, con los mismos efectos que las leyes otorgan a los documentos firmados autógrafamente y, por otra, que el aludido instituto podrá conservar en dichos medios la información presentada en formatos impresos. Por tanto, para que los estados de cuenta individuales, que son impresiones o registros de la información que obra en dispositivos magnéticos o electrónicos, tengan suficiente valor probatorio para acreditar la relación laboral entre el patrón y los trabajadores a que se refieren, es necesario evaluar, entre otros aspectos, los requisitos que exige el segundo párrafo del artículo 210-A del Código Federal de Procedimientos Civiles, aplicado supletoriamente, que son, en primer lugar,

la fiabilidad del método en que se encuentre o almacene la información, es decir, donde se genere, comunique, reciba o archive; en segundo, de ser posible, que se atribuya el contenido de la información al patrón; y en tercero, que ésta sea accesible para su posterior consulta. Por consiguiente, debe acreditarse que efectivamente dicha información fue aportada por el patrón, ya sea conservando los formatos impresos autorizados o su resguardo en medios magnéticos o electrónicos, tal como lo señala el artículo 4 del citado reglamento, o bien, corroborar con el número patronal de identificación electrónica correspondiente (equivalente a la firma electrónica) que la información enviada por medios electrónicos fue efectivamente aportada por el patrón, pues en términos del invocado artículo 5, sólo los trámites en que se utilice ese número producirá los mismos efectos que los documentos firmados autógrafamente.”.

- **Localización:** Novena Epoca, Instancia: Primera Sala, Fuente: Semanario Judicial de la Federación y su Gaceta, XXV, Marzo de 2007, Página: 30, Tesis: 1a./J. 27/2007, Jurisprudencia, Materia(s): Común.

“CONSTANCIAS ENVIADAS POR FAX ENTRE LOS ÓRGANOS DEL PODER JUDICIAL DE LA FEDERACIÓN. SI ESTÁ CERTIFICADA LA HORA Y FECHA DE SU RECEPCIÓN, ASÍ COMO EL ÓRGANO QUE LAS REMITE POR EL SECRETARIO DE ACUERDOS DEL TRIBUNAL JUDICIAL QUE LAS RECIBE, TIENEN PLENO VALOR PROBATORIO. El artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo en términos de lo previsto en el diverso artículo 2o. de esta Ley, reconoce como medios de prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología, y establece que su fuerza probatoria está sujeta a la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Ahora bien, entre los medios de comunicación electrónica se encuentra el denominado fax, que es un medio de transmisión de datos que emplea la red telefónica, por el cual se envía un documento que se recibe por el destinatario en copia fotostática; de ahí que las constancias transmitidas por este medio, entre los órganos del Poder Judicial de la Federación, si están certificadas por el secretario de Acuerdos del tribunal judicial al que se transmite el mensaje, sobre la hora y fecha de recepción del fax y la persona del órgano jurisdiccional federal que lo remitió, tienen pleno valor probatorio, por ser confiable el medio en que fueron comunicadas dichas constancias, ya que tiene un grado de seguridad similar al de la documentación consignada en papel, además de que es identificable la persona a quien se atribuye su contenido y pueden verificarse tanto el origen de la documentación como su texto; pues en la actualidad los citados órganos se encuentran comunicados

electrónicamente, por distintos medios, lo que permite corroborar los datos del fax recibido.”.

- **Localización:** Novena Epoca, Instancia: Tribunales Colegiados de Circuito, Fuente: Semanario Judicial de la Federación y su Gaceta, XXIV, Octubre de 2006, Página: 1496, Tesis: XXI.2o.P.A.32 K, Tesis Aislada, Materia(s): Común.

“PRUEBA DE INSPECCIÓN. DEBE DESECHARSE CUANDO LOS PUNTOS PROPUESTOS PARA SU DESAHOGO PUEDAN SER COMPROBADOS A TRAVÉS DE LA DOCUMENTAL, ENTENDIDA COMO LA INFORMACIÓN GENERADA O COMUNICADA QUE CONSTE EN MEDIOS ELECTRÓNICOS O EN CUALQUIER OTRA TECNOLOGÍA, QUE PUEDE SER REPRODUCIDA, NO SOLAMENTE EN PAPEL SINO TAMBIÉN EN ALGÚN DISQUETE O DISCO ÓPTICO. La base de datos existente en el sistema de cómputo de alguna dependencia oficial, constituye, en sentido amplio, una documental, atendiendo a que el artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, por disposición de su artículo 2o., segundo párrafo, señala que se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. En ese contexto, resulta correcto desechar la prueba de inspección cuando los puntos materia de su desahogo tienen como propósito demostrar hechos susceptibles de ser comprobados a través de la prueba documental, entendida ésta como la información que puede ser reproducida, no exclusivamente en papel, sino también en algún disquete o disco óptico, en el cual se logre grabar la información solicitada por el quejoso para efectos de exhibirlos como prueba en el juicio de amparo, de conformidad con el artículo 152 de la Ley de Amparo.”.

- **Localización:** Novena Epoca, Instancia: Tribunales Colegiados de Circuito, Fuente: Semanario Judicial de la Federación y su Gaceta, XXII, Octubre de 2005, Página: 2471, Tesis: I.7o.A.410 A, Tesis Aislada, Materia(s): Administrativa.

“RECIBO DE PAGO ELECTRÓNICO. VALOR PROBATORIO DE LA DOCUMENTAL IMPRESA CORRESPONDIENTE. El artículo 210-A del Código Federal de Procedimientos Civiles reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología, condicionando su valor a la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada, y en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. De esta manera,

el legislador, ante los avances de la tecnología, contempló la posibilidad de que en los juicios seguidos ante los tribunales se exhibieran y valoraran elementos probatorios distintos a los convencionales, tales como testimoniales, periciales, documentos, entre otros; consecuentemente, la información generada por la vía electrónica (internet, comercio electrónico y análogos), tiene un respaldo legislativo, a efecto de crear seguridad jurídica en los usuarios de tales servicios. Así, la valoración del material probatorio en comento no debe sujetarse a las reglas convencionales de justipreciación, sino al apartado específico del numeral en estudio; de esta manera, un recibo de pago de impuestos realizado electrónicamente no carece, por tal circunstancia, de eficacia probatoria, ya que lo que se habrá de tomar en consideración, en su momento, son los datos que corroboren su fiabilidad, como son el código de captura y sello digital, y no elementos ajenos a la naturaleza de los documentos electrónicos, tales como si se trata del original de una impresión.”.

- **Localización:** Novena Epoca, Instancia: Tribunales Colegiados de Circuito, Fuente: Apéndice 2002, Tomo IV, Civil, P.R. TCC, página 113, que es del tenor siguiente:

“INFORMACIÓN PROVENIENTE DE INTERNET. VALOR PROBATORIO. El artículo 188 del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, en términos de lo previsto en el diverso artículo 2o. de este ordenamiento legal, dispone: "Para acreditar hechos o circunstancias en relación con el negocio que se ventila, pueden las partes presentar fotografías, escritos o notas taquigráficas, y, en general, toda clase de elementos aportados por los descubrimientos de la ciencia."; asimismo, el diverso artículo 210-A, párrafo primero, de la legislación que se comenta, en lo conducente, reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquiera otra tecnología; ahora bien, entre los medios de comunicación electrónicos se encuentra "internet", que constituye un sistema mundial de diseminación y obtención de información en diversos ámbitos y, dependiendo de esto último, puede determinarse el carácter oficial o extraoficial de la noticia que al efecto se recabe, y como constituye un adelanto de la ciencia, procede, en el aspecto normativo, otorgarle valor probatorio idóneo.”.

- **Localización:** Novena Epoca, Instancia: Tribunales Colegiados de Circuito, Fuente: Semanario Judicial de la Federación y su Gaceta, XVI, Agosto de 2002, Página: 1279, Tesis: V.3o.9 C, Tesis Aislada, Materia(s): Civil.

“DOCUMENTAL CONSISTENTE EN INFORMACIÓN EXTRAÍDA DE INTERNET. EN CUANTO DOCUMENTO INNOMINADO, CON BASE EN EL ARBITRIO JUDICIAL, PUEDE

ASIGNÁRSELE VALOR INDICIARIO. El Código de Comercio establece en sus artículos 1237, 1238 y 1297, respectivamente, cuáles son los instrumentos públicos, los privados y los simples; asimismo, en los diversos artículos 1277, 1279 y 1284 de la legislación en cita, refiere las presunciones humanas; ahora bien, de la interpretación armónica de los citados artículos se infiere que el documento que contiene información referente a las tasas de intereses recabadas de "internet", como medio de diseminación y obtención de información, el citado instrumento no constituye un documento público pues, además de no ser un documento original, no contiene sello o alguna otra característica que señale la ley para darle el carácter de público, ni tampoco puede considerarse como documento privado, porque no constituye un documento original, conforme lo requiere el artículo 1242 de la ley en consulta; en consecuencia, de ello se deduce que dicho instrumento sólo puede ser considerado como documento simple y, por tanto, innominado; de suerte que si éste es un medio de prueba reconocido por la ley y no se demostró que la información contenida en dicho documento sea incongruente con la realidad, de ello deriva que es apto para integrar la presuncional humana, con observancia, además, del artículo 1205, del Código de Comercio, que señala: "Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad."; de ahí que su valor quede al arbitrio del juzgador como indicio, y como tal deban atenderse los hechos que con dicho instrumento se pretendan demostrar, en concordancia con los demás medios de convicción que obren en autos."

En el panorama internacional, las Naciones Unidas, por conducto de la UNCITRAL, ha emitido un documento, titulado *Legal Value of Computer Records*, en el que expresa que las normas o reglas concernientes a las pruebas relativas a los registros de computadora (documentos electrónicos), no deben suponer un obstáculo para el uso de las tecnologías emergentes tanto a nivel doméstico como internacional, y señala que los países deben superar los problemas que genera el lenguaje empleado.

Por su parte, en Estados Unidos, estado de UTAH en específico, quien ha sido el primero en legislar sobre la materia, el 1 de mayo de 1995 sancionó la "UTAH Digital Signature Act"; la cual, ha sido referencia obligada para los demás estados, en cuanto al sistema regulatorio de la firma digital, junto con la Digital Signature Guidelines (Guía de Firma Digital), publicada en octubre de 1995 por el Comité de

Seguridad de la Información de la Asociación Americana de Abogados; dando como resultado que el 1 de octubre de 2000, entrara en vigor la primera ley nacional sobre firmas digitales.

Italia, conformó el Reglamento de actos, documentos y contratos en forma electrónica aprobada el 5 de agosto de 1997.

Por su parte Francia, país pionero en este campo, el 12 de junio de 1980, sancionó la ley 80/525, reformando el artículo 1348 del Código Civil, en el cual se estableció que el documento electrónico tendría el mismo valor probatorio que el documento en soporte de papel escrito y firmado, cuando cumpliera con determinados requisitos, como son inalterabilidad y durabilidad. Mediante la Ley número 2000-230 de 13 de marzo de 2000, nuevamente fue reformado dicho ordenamiento, introduciendo modificaciones al capítulo VI (De la prueba de las obligaciones y del pago), en sus artículos 1315, inciso I y artículo 1316, incisos 1 a 4, refiriéndose a la prueba de las nuevas tecnologías de la información y de la firma electrónica.

En España, se ha legislado sobre la validez del documento electrónico y de las comunicaciones telemáticas como prueba documental. El Real Decreto-Ley 14/1999, establece un régimen específico aplicable a las relaciones telemáticas. En 2003 se publicó la ley de firma electrónica, la ley 59/2003, la cual introduce algunas modificaciones, reformas, mejoras y supresiones, en diversas cuestiones reguladas en aquél Decreto-Ley.

1.3.5. Gobierno digital y ciberjusticia.

El gobierno digital o *e-government*, es una nueva forma de gobierno basada en un concepto de gestión que fusiona el empleo de las tecnología de la información y comunicación, con modalidades de gestión y administración.⁵⁷

⁵⁷ Cfr. Téllez Valdés, Julio, ob cit, pág., 35.

El gobierno de Chile aplicó ésta nueva forma de gobierno a política de Estado, atento a los siguientes objetivos:

- Aumentar niveles de eficiencia en la gestión pública.
- Disminuir significativamente costos de transacción y coordinación en la interacción entre entes públicos.
- Generar incentivos y prácticas que faciliten modalidades de gestión innovadoras y creativas.
- Agregar mayor valor público como horizonte permanente de las actividades del sector.
- Superar de modos constantes los grados de transparencia de esas actividades, en aquello que un servidor conceptualizó como “cibertransparencia.”.
- Acelerar el tránsito hacia una administración centrada en el ciudadano.
- Mejorar la calidad de los servicios que se proveen y las modalidades de provisión.
- Facilitar el cumplimiento de las obligaciones de los ciudadanos.
- Disminuir de manera significativa los costos de transacción entre ciudadanos y agentes públicos.
- Suprimir paulatinamente barreras, ineficiencias e irracionalidad en la interacción entre particulares y sector público.
- Transformar al sector público en facilitador del crecimiento y de distribuciones más equitativas de los niveles de bienestar social.⁵⁸

Según el autor Rodrigo Sandoval Almazán, “el debate para definir al gobierno electrónico se centra en la ausencia de límites de su acción, en ser visto como una herramienta para mejorar los trámites y servicios y la posibilidad de gobernar la red y de ser un instrumento que promueva la democracia y los valores democráticos en las sociedades.”⁵⁹

⁵⁸ Cfr. *Ibidem*, p.p. 35 y 36.

⁵⁹ *Ibidem*, pág. 36.

A la luz de esta nueva forma de gobierno han nacido diversos conceptos en materia de administración, democracia y gobierno.

La ***e-administración*** o **administración electrónica**, hace referencia a aquellos mecanismos electrónicos que permiten la prestación de servicios públicos de la administración a ciudadanos y a empresas.

La ***e-democracia*** o **democracia electrónica**, permite la participación ciudadana en las decisiones políticas, a través de las TIC (nuevas tecnologías de información y comunicación), como lo es el voto electrónico.

El ***e-gobierno*** o **gobierno electrónico**, abarca todos los servicios en línea en la prestación de servicios públicos.⁶⁰

La **justicia**, significa, dar a cada quien lo que le corresponde. La ***ciberjusticia***, es impartida por cibertribunales, en donde se ventilan los juicios en línea, con apoyo de las tecnologías de información y comunicación.

Como ejemplos de estos cibertribunales, en materia de comercio electrónico, se encuentran los siguientes:

e-Resolution. Fundado en 1999. Se utiliza para la solución en línea de litigios relativos a los nombres de dominio. Inauguró su primer servicio de solución en línea de deferencias el 1 de enero de 2000, cuando recibía la acreditación de la Corporación Internet para Nombres y Números Asignados (ICANN). La plataforma tecnológica de *eResolution* ha permitido resolver varios cientos de asuntos con alcance mundial.

Cibercorte en Michigan. Surge a través del gobernador John Engler, quien firmó a principios de 2002, un decreto para establecer en Michigan, Estados Unidos, una cibercorte independiente para los casos relativos a empresas de alta tecnología. Es una nueva forma de llevar los procesos; ello, en línea, donde surgen las

⁶⁰ Cfr. *Ibidem*, p.p. 36 y 37.

teleconferencias, o conferencias vía e-mail, asimismo, las audiencias pueden celebrarse en cualquier momento del día.

Cibertribunal de Lieja (Bélgica). Proyecto fue propuesto a la Fundación Rey Baudouin a finales de 2000, a iniciativa de la barra de abogados de dicha ciudad (Justicia en movimiento).

61

Por otro lado, existen otras formas de solución de conflictos en la materia, como lo son: la conciliación, la mediación y el arbitraje, en donde han surgido proyectos fundados por diversos organismos internacionales, algunos de los cuales actualmente se encuentran en operación, a saber:

Virtual Magistrate. En marzo de 1996 se inauguró este proyecto, un servicio de arbitraje en línea resultante de la colaboración entre *Cyberspace Law Institute* (CLI) y el *National Center for Automated Information Research* (NCAIR). Su objetivo, era estudiar la manera de resolver las diferencias entre un usuario y un operador de redes, o entre usuarios. El ámbito de aplicación se limitaba a los conflictos generados por mensajes o ficheros con contenido ilícito. El procedimiento de arbitraje era voluntario y se efectuaba esencialmente por correo electrónico. Se denomina arbitraje contractual, en virtud de que surtía algunos efectos obligatorios, pero no tenía efectos ejecutorios con arreglo a las legislaciones y tratados sobre la materia. Este proyecto se prosigue bajo los auspicios de la Universidad Chicago Kent.

On line Ombuds Office (Oficina de Mediadores en Línea). Es una iniciativa del Center for Information Technology and Dispute Resolution de la Universidad de Massachusetts. Desde 1996, esta oficina ofrece sus servicios de mediación particularmente en asuntos relacionados a litigios entre miembros de un grupo de debate, competidores, entre proveedores de acceso a Internet, y relacionados con propiedad intelectual. El proyecto se prosigue en la actualidad.

⁶¹ Cfr. *Ibidem*, p.p. 45,50-51.

CyberTribunal. Era un proyecto experimental elaborado por el Centre de Recherche en Droit Publique (CRDP, por sus siglas en francés), de la Universidad de Montreal, en septiembre de 1996. Era el de mayor apertura. No se erigía un juez, sino de moderaba el diálogo entre las partes a través de la mediación. El proyecto terminó en diciembre de 1999.

Square Trade. Fundado en 1999. Funciona en mayor apego en el sector de comercio electrónico entre consumidores C2C. El procedimiento es amistoso, en el sentido de su informalidad. Primeramente, el comprador o el vendedor presentan una queja a Square Trade, recopilando toda la información pertinente en un formulario electrónico. Seguido, se notifica a la contraparte por correo electrónico. Si se presenta una respuesta, este servicio permite a las partes el acceso a formularios en un sitio protegido, mediante contraseñas y nombre de usuario. En esta etapa las partes pueden tratar de resolver el litigio de forma amistosa, de lo contrario, podrán pedir a Square Trade, que designe un mediador, en cuyo caso deberán pagar un honorario bastante modesto. En caso de un arreglo, con o sin ayuda del mediador, la diferencia quedará solventada y se comunicará a las partes un documento en el que se consigna el acuerdo.

Centro de Arbitraje y Mediación de la Organización Mundial de la Propiedad Intelectual. Tiene su sede en Ginebra, Suiza, y fue creado en 1994. Es una dependencia administrativa de la Oficina Internacional de la Organización Mundial de la Propiedad Intelectual (OMPI) y miembro de la Federación Internacional de Instituciones de Arbitraje Comercial (IFCAI). Ofrece servicios de arbitraje y mediación en relación con controversias internacionales comerciales entre partes privadas. Se le ha reconocido como uno de los principales proveedores de servicios de solución de controversias referentes a las controversias que plantean el registro y el uso de los nombres de dominio, y lo relacionado con la solución de controversias en materia de propiedad intelectual e Internet. Actualmente, este centro de arbitraje presta sus servicios al Application Service Provider Industry Consortium, consorcio internacional no lucrativo formado por más de 400 de las principales empresas mundiales dedicadas a las tecnologías de la información, a fin de elaborar

prácticas y directrices para prevenir y solucionar las controversias internacionales. El centro recibe apoyo de una comisión consultiva y del Consejo de Arbitraje de la OMPI, ambos integrados por expertos de alto nivel.

Instituto para la Resolución de Conflictos (CPR). Fundada en 1999; es una alianza no lucrativa constituida por organismos multinacionales y despachos prestigiosos para ofrecer a empresas e instituciones públicas una alternativa. Formado por 500 asesores legales de las mayores empresas, socios de los mejores despacho, catedráticos notables e instituciones públicas seleccionadas. Su manera de actuar es a través de los llamados paneles de neutralidad y mediación. Incluye en su programa extensas publicaciones: libros, videos, modelos de procedimiento de resolución de conflictos y herramientas prácticas en más de 20 áreas tanto sustantivas como procedimentales, así como modelos formales y sus cláusulas respectivas.

Foro de Arbitraje Nacional (NAF). Fundado en 1986 en Minneapolis, Minnesota, notable por su neutralidad en la toma de decisiones y la aplicación de leyes sustantivas para resolver casos de arbitraje. Obtuvo la aprobación como un proveedor de servicio para la resolución de disputas por ICANN el 23 de diciembre de 1999.

La **Directiva Europea sobre Comercio Electrónico**. Hace referencia a la solución extrajudicial de litigios y dispone en su apartado primero que los Estados miembros velarán, para que en el caso de desacuerdo entre un prestador de servicios de la sociedad de la información y el destinatario de aquéllos, su legislación permita utilizar de manera efectiva mecanismos de solución extrajudicial, incluso mediante vías electrónicas adecuadas.⁶²

1.3.6. Delitos informáticos.

⁶² Cfr. Téllez Valdés, Julio, ob. cit, págs. 43-51.

El delito informático, es el acto u omisión que sancionan las leyes penales, relacionados con las técnicas destinadas al tratamiento lógico y automatizado de la información. El bien jurídico que tutela es el patrimonio.

El delito informático es “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.”⁶³

La Comisión Europea señala un concepto amplio de delito informático, al indicar lo siguiente: “En esta Comunicación se aborda la delincuencia informática en el sentido más amplio; cualquier delito que de alguna manera implique el uso de tecnología de información. Sin embargo, existen distintos puntos de vista sobre lo que constituye “delincuencia informática”. Suele utilizarse indistintamente los términos “delincuencia informática”, “delincuencia relacionada con la información”, “delincuencia de alta tecnología” y “delincuencia cibernética.”⁶⁴

Se distingue el medio y el fin, para encuadrar un acción dolosa o imprudente dentro del este tipo de delitos, donde “el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática.”⁶⁵

Propiamente en nuestra legislación, así como en las legislaciones de otros países, no se encuentra tipificado este delito con el nombre de “delito informático”; sin embargo, se han tipificado las diversas conductas antijurídicas que encuadran a este delito; asimismo, se han establecido los elementos objetivos, normativos y objetivos que integran el cuerpo del delito y la probable responsabilidad.

⁶³ Davara Rodríguez, Miguel Ángel, ob. cit, pág. 356.

⁶⁴ Ibidem, p.p. 357.

⁶⁵ Ibidem, p.p. 358.

Las características comunes de este tipo de delito, son la rapidez y acercamiento, en tiempo y espacio para su comisión, la facilidad para encubrir el hecho, y la facilidad para borrar las pruebas.

Se ha clasificado este delito a través de tres categorías, a saber:

1. Los que utilizan la tecnología electrónica como método. Son conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito. Como ejemplo de este tipo de delito se encuentran, los métodos conocidos como caballo de Troya, técnica de salami, y bombas lógicas. El método *caballo de Troya*, consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. La *técnica de salami*, es la variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa. Las *bombas lógicas*, cuyo efecto es un daño –borrado o destrucción de ficheros- en tiempo posterior –con retardo- al momento de su introducción.

2. Los que utilizan la tecnología electrónica como medio. Son conductas criminógenas en donde para la comisión del delito utilizan la computadora como medio o símbolo. Ejemplos, de estos se encuentran: la falsificación de documentos vía computarizada (tarjetas de crédito, tarjetas de debito, cheques, etc.); variación de los activos y pasivos en la situación contable de las empresas; planeación o simulación de delitos convencionales (robo, fraude); lectura, sustracción o copiado de información confidencial; inclusión de instrucciones que provocan interrupciones en la lógica interna de los programas a fin de obtener beneficios; alteración en el funcionamiento de los sistemas; acceso a áreas informatizadas en forma no autorizada; intervención del proceso en las líneas de comunicación de datos o teleproceso; introducción de datos falsos mediante manipulación de los datos que son introducidos en un ordenador en el proceso de entrada al sistema; simulación de actividades mediante la utilización del sistema informático para conocer la estructura

lógica y de funcionamiento de una determinada actividad o los resultados y previsiones de una empresa, etcétera.

3. Los que utilizan la tecnología electrónica como fin. Son conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla; entre otros se encuentran los siguientes: programación de instrucciones que producen un bloqueo total al sistema; destrucción de programas de cualquier método; daño a la memoria; atentado físico contra la máquina o sus accesorios (discos, cintas, terminales); sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados; y, secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje por pago de rescate.⁶⁶

La Comisión de las Comunidades Europeas, en su comunicación “Seguridad de las redes y de la información: propuesta para un enfoque político europeo”, propuso la siguiente clasificación:

a) ***Acceso no autorizado a sistemas de información.*** Incluye el concepto de “piratería informática”, la cual consiste en tener acceso de manera no autorizada a una computadora o a una red de computadoras, que van desde el mero uso de informaciones internas hasta ataques directos y la interceptación de contraseñas. Se realiza generalmente pero no siempre con una intención dolosa de copiar, modificar o destruir datos. La corrupción deliberada de sitios de Internet o el acceso sin previo pago a servicios restringidos, puede constituir uno de los objetivos del acceso no autorizado.

b) ***Perturbación de los sistemas de información.*** Refiere al ataque de tipo de denegación de servicios (Dds), el cual, es en cierta medida análogo a inundar las máquinas de fax con mensajes largos y repetidos. Los ataques del tipo de denegación de servicio tiene por objeto sobrecargar los servidores o los proveedores de servicios

⁶⁶ Cfr. Téllez Valdés, Julio, ob. cit, p.p. 190.

Internet (PSI) con mensajes generados de manera automática. Otros tipos de ataques, pueden consistir en perturbar los servidores que han funcionado el sistema de nombres de dominio (DNS), y los ataques contra los “encaminadores”. Estos ataques han sido perjudiciales para algunos sitios web prestigiosos como los portales, que según estudiosos, causan daños estimados en varios centenares de millones de dólares, sin contar el perjuicio no cuantificable en términos de reputación.

c) ***Ejecución de programas informáticos perjudiciales que modifican o destruyen datos.*** El tipo más conocido es el “virus”. Los virus “I Love you”, “Melissa” y “Kournikova” son algunos ejemplos conocidos. Otros ejemplos son, las “bombas lógicas”, que pueden permanecer inactivos hasta que se desencadenan por algún motivo y causan graves daños al modificar o destruir datos, y “caballos de Troya”. Existen otros tipos de programas que dañan la computadora, mientras que otros utilizan la PC para atacar otros elementos de red.

d) ***Intercepción de las comunicaciones.*** Afecta los requisitos de confidencialidad e integridad de los usuarios, se denominan *sniffing* (intromisión).

e) ***Declaraciones falsas.*** Usurpación de la identidad de otra persona en Internet y utilizarla con agravio, se llama *spoofing* (modificación de datos).⁶⁷

La Organización de las Naciones Unidas, ha estimado en el “Manual de las Naciones Unidas para la prevención y control de delitos informáticos”, que se requiere la cooperación internacional en el área de los delitos informáticos, en virtud de la naturaleza transnacional de dichos delitos, y reconoce todo un listado de los tipos de delitos en este ámbito, a saber:

1. Fraudes cometidos mediante manipulación de computadoras.

- *Manipulación de los datos de entrada.* Conocido también como sustracción de datos; representa el delito informático más

⁶⁷ Téllez Valdés, Julio, ob. cit, p.p 191.

común ya que es fácil de cometer y difícil de descubrir. Puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la base de adquisición de éstos.

- *Manipulación de programas.* El delincuente tiene habilidades técnicas de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas. Un método común utilizado es el denominado “*caballo de Troya*”, el cual, consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
- *Manipulación de datos de salida.* Para efectuarla se fija un objetivo al funcionamiento del sistema informático. El ejemplo más común es la falsificación de instrucciones para la computadora en la base de adquisición de datos en los cajeros automáticos. Se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y las de crédito.
- *Fraude efectuado por manipulación informática.* Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica denominada “*técnica del salami*”, en la cual “rodajas muy finas”, apenas perceptibles, de transacciones financieras, se sacan repetidamente de una cuenta y se transfieren a otra.

2. Falsificaciones informáticas

- Como *objeto*. Cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como *instrumento*. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopadoras en color base de rayos láser surgió una nueva generación de falsificaciones. Estas fotocopadoras pueden hacer copias de alta resolución, modificar documentos e incluso componer documentos falsos sin tener que recurrir a un original.
- *Acceso no autorizado a sistemas o servicios*. Ocasionado por los piratas informáticos (hacker), o bien por sabotaje o espionaje informático, de los que se encuentran:
 - *Piratas Informáticos o hackers*. Es la persona que accede a una computadora de forma no autorizada e ilegal, valiéndose de medios informáticos y de telecomunicaciones. Su motivación es el simple deseo de quebrantar el sistema como desafío propio. A menudo se hacen pasar por usuarios legítimos del sistema.
 - *Crackers*. Toda persona que por medios informáticos y de telecomunicaciones, accede a sistemas de información que le son vedados, con la intención de provocar un daño o apoderarse indebidamente de información.
 - *Phreaker*. Es la persona que para llevar a cabo la actividad de hacker o de cracker, utiliza indebidamente líneas telefónicas, que más allá del valor de los pulsos telefónicos utilizados, su motivación es evitar ser rastreado por el software específico diseñado para tal efecto.

- *Reproducción no autorizada de programas informáticos de protección legal.* Relativo a la propiedad intelectual, cuya conducta trastoca los programas de ordenador, a la documentación técnica, manuales de uso, versiones sucesivas y programas derivados. Algunas jurisdicciones han tipificado esta actividad y la han sometido a sanciones penales.

3. Daños o modificaciones de programas o datos computarizados.

- *Sabotaje informático.* Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que utilizan para ello, son: virus, “gusanos”, y bomba lógica o cronológica, las cuales se describen a continuación: *Virus*, es una serie de claves programáticas que pueden adherirse a los programas informáticos y propagarse a otros. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como mediante el método caballo de Troya. “*Gusanos*”, se fabrican de forma análoga al virus con miras a infiltrarlos en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. *Bomba lógica o cronológica.*, exige habilidades especializadas ya que requiere programar la destrucción o modificación de datos en un futuro. A diferencia de los virus o los “gusanos”, las bombas lógicas son difíciles de detectar antes de que exploten. Su detonación puede programarse para que cause el máximo daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. También se utiliza como medio de extorsión.⁶⁸

⁶⁸ Cfr. *Ibidem*, p.p. 193.

Existen formas de control implementados, en específico, en el área laboral, que inciden en la función preventiva, cuyo propósito es tener certeza de la fidelidad del personal que labora dentro de las áreas informáticas de trabajo, lo que reduce de manera notable las conductas atípicas; considerándose básicamente las siguientes: 1. *mesa de valores*; 2. elaboración de exámenes; 3. establecimiento de un código ético de carácter interno en las empresas; 4. adopción de estrictas medidas en el acceso y control de las áreas informáticas de trabajo; 5. capacitación del personal informática; identificación del personal; y, 6. rotación en el uso de claves de acceso al sistema; entre otras.

Respecto de la **mesa de valores** cabe destacar que los principios y valores consolidan una nación hacia la dirección correcta; tales como: **honestidad; esfuerzo; humildad; transparencia; paciencia; ahorro; trabajo duro; dominio propio;** etcétera; que hacen falta enseñar, y ser practicados. Por ello, la propuesta de mesas de valores en los centros de trabajo, en donde se interactúe con otros, y puedan ser observados y evaluados estos principios por la propia persona, a través de su práctica diaria en todas las áreas que desarrolla.

En el marco internacional, cabe mencionar algunas naciones como Estados Unidos, Alemania, Austria, Gran Bretaña Holanda, Francia, España, y México, se han destacado en la labor de legislar sobre esta materia, surgiendo así criterios adoptados por sus órganos jurisdiccionales, de acuerdo a la dinámica que representa esta materia.

Estados Unidos, adoptó en 1994 el “Acta Federal de Abuso Computacional, que modificó el Acta de Fraude y Abuso Computacional de 1986”.

Alemania, sancionó en 1986 la “Ley contra la Criminalidad Económica”, que se refiere a delitos como: espionaje de datos, fraude informático, alteración de datos, y sabotaje informático.

En Austria, la ley de reforma del código penal, sancionada el 22 de diciembre de 1987, en el artículo 148 sanciona a aquellos que con dolo causen un perjuicio

patrimonial a un tercero de tal manera que influyan en la elaboración de datos automática mediante el diseño del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.

En Gran Bretaña, en 1991 comenzó a regir en este país la “Computer Misuse Act” (Ley de Abusos Informáticos). Esta ley sanciona la alteración de datos informáticos, y su tentativa.

En Holanda, el 1 de marzo de 1993, entró en vigor la “Ley de Delitos Informáticos”, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), ingeniería social (convencimiento de entregar información que en circunstancias normales no entregaría), y la conculcación de virus.

En Francia, se dictó en enero de 1998, la ley relativa al fraude informático, la cual prevé penas por la intromisión fraudulenta que suprima o modifique datos.

En España, se crea el Nuevo Código Penal de España, que sanciona en diverso dispositivo 264-2, al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

En nuestro país, si bien no se encuentra tipificado el “delito informático” con tal término, lo cierto es que, sí se encuentran tipificadas como delito grave, diversas conductas antijurídicas que convergen a este tipo penal.

El Código Penal Federal, en su Capítulo II, Título Noveno, tiene como título “**Acceso ilícito a sistemas y equipos de informática**”; mismo que fue adicionado con los artículos que lo integran, publicados en el Diario Oficial de la Federación el 17 de mayo de 1999; a saber:

“**Artículo 211 bis 1.** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.- - - Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.”.

“**Artículo 211 bis 2.** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.- - - Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.- - - A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.”.

“**Artículo 211 bis 3.** Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.”.- - - Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.- - - A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que

contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.”.

“**Artículo 211 bis 4.** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.- - Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.”.

“**Artículo 211 bis 5.** Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.- - Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.”.- - Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.”.

“**Artículo 211 bis 6.** Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.”.

“**Artículo 211 bis 7.** Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.”.

Por su parte, el Código Penal del Distrito Federal, establece en los artículo 230 y 231, fracción XIV, en su parte conducente, lo siguiente:

“**Artículo 230.** Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán:...”.

“**Artículo 231.** Se impondrán las penas previstas en el artículo anterior, a quien: . . . **XIV.** Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución.”

De estos ordenamientos, se colige que México ha dado un avance considerable en la regulación del llamado doctrinalmente “delito informático”; no obstante, en cuanto hace a otras conductas antijurídicas, aún falta regular de manera más firme; tal es el caso de la pornografía; la cual trastoca la integridad de una nación, especialmente, la familia.

Un caso que cabe distinguir, es la ley promovida por el senador Jim Exon en el año de 1995, llamada **Ley de la Decencia en las Comunicaciones de Estados Unidos**, la cual fue ratificada como ley federal el 8 de febrero de 1996; que provocó una reacción inmediata en su contra por las asociaciones “pro derechos civiles” en la Unión Americana. Esta ley prohibía el acceso a sitios con material relacionado con artículos y órganos sexuales o excretorios, considerados manifiestamente ofensivos e indecentes. Asimismo, exponía que cualquier ciudadano que exhibiera en una página web opiniones o imágenes de contenido indecente u ofensivo y que fueran vistas por un menor de edad, podría ser sancionado con una pena de hasta dos años de prisión.

Algunos de los principales postulados de esta ley, eran castigar a cualquier persona que creara, hiciera, solicitara o iniciara en medios de telecomunicación nacionales o extranjeros, cualquier comentario, solicitud, sugerencia o propuesta, imagen u otra comunicación obscena, lujuriosa, sucia o indecente; que pretenda molestar, abusar, amenazar, acosar u hostilizar a otra persona. Esta ley fue impugnada judicialmente por la American Civil Liberties Unión (ACLU, Asociación de Libertades Civiles de Estados Unidos), que sostuvo su inconstitucionalidad por la “violación” de libertad de expresión. En junio de 1997 fue declarada “atentatoria contra la libertad de expresión” consagrada en la Primera Enmienda y, en consecuencia, inconstitucional por la Suprema Corte de esa nación.⁶⁹

Esta ley es un modelo a seguir en México, ejemplo de salvaguarda y protección de los derechos y valores del hombre. Anhele un día lleguemos a ese modelo valiente de legislar.

Si bien, en nuestro país el Código Penal Federal, así como los códigos penales de las entidades federativas como Baja California, Chiapas, Durango, Guerrero, Jalisco, Oaxaca, Puebla y Zacatecas, y el Distrito Federal, han legislado sobre este tema; no ha sido con la firmeza de dicha ley estadounidense de 1995.

El Código Federal Penal, establece en su artículo 202, lo siguiente:

“Artículo 202. Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de

⁶⁹ Cfr. Téllez Valdés, Julio, ob. cit, p.p. 105.

cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.- - - A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito.- - - La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores”. (resalto)

Por su parte, el artículo 187, del Código Penal para el Distrito Federal, establece lo siguiente:

“**Artículo 187.** Al que procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio a una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de videgrabarlos, audiograbarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, electrónicos, o sucedáneos se le impondrá de siete a catorce años de prisión y de dos mil quinientos a cinco mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales mencionados...”. (resalto)

“No llamemos a lo malo bueno”.

Desde una interpretación desde el elemento “gramatical, lingüístico o filológico”⁷⁰, dichos numerales omiten los demás supuestos o conductos que encuadran a este tipo penal; esto es, cuando es persona mayor de 18 años, quien aún

⁷⁰ Cisneros Farias, Germán, *La Interpretación de la Ley*, editorial Trillas, Sociedad Anónima de Capital Variable, México 2000, pág. 46.

teniendo capacidad de comprender el significado del hecho, y que puede resistir la conducta, ejecuta los actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de que sean expuestos o exhibidos en video, fotografía, anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo electrónicos o sucedáneos.

Por tanto, son autores de este delito tanto el que procura o facilita a estas personas mayores de 18 años, a realizar dichas conductas antijurídicas, para exhibirlos en los diversos medios mencionados, así como a aquel que ejecuta dichos actos sexuales o de exhibicionismo.

En conclusión, **se debe castigar** a todo aquel que procure, obligue, facilite o induzca, por cualquier medio, a **“cualquier persona”**, a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos; **así como a aquel que tenga participación directa o indirecta en la ejecución de dichos actos sexuales o de exhibicionismo**; con excepción, de las personas mencionadas en el numeral 202 del Código Federal Penal.

En virtud de que esta problemática transgrede los valores de una sociedad, ha generado que la propia sociedad civil, en específico, las familias, en conjunto con algunas empresas, marquen pautas en Internet a través de la “autocensura”.

Son muchas las compañías que ofrecen portales gratuitos y prohíben la publicación de imágenes pornográficas y grupos de discusión rechazan el uso del lenguaje impropio, lo que genera principios y valores, y por ende, un desarrollo y estructuras de la red armónicos, transparentes y edificantes.

Francia, es uno de los pioneros en introducir códigos deontológicos o de buena conducta en la red, con sus “netiquetes” o reglas de etiqueta en la red. En

Inglaterra se han adoptado mecanismos de autorregulación, en donde se han originado códigos de conducta y organismos como la Safety Net Foundation, la cual mantiene una línea directa para recibir denuncias de contenidos o actividades que se consideren ilícitos.

Otro mecanismo, es el llamado “programas filtro”, o de selección de contenidos ilícitos, donde es posible permitir la libre circulación de información, con la restricción de aquellos cuyo contenido sea ilícito o no edificante; se maneja a nivel del proveedor o del propio usuario.

“Discernir para elegir lo que conviene, y desechar lo que no conviene”. Sólo falta la participación del Estado, quien a través de las políticas que establezca, se consoliden estas medidas de seguridad, y contribuya a alcanzar el propósito edificante por lo que fue creado Internet, y sancione de manera firme, a aquellos actores que promuevan o participen en la exhibición de información cuyo contenido es ilícito.

1.3.7. Aplicación actual en México.

Ha sucedido una renovación en el país en torno a la informática, aparejado esto con el fenómeno de la red mundial llamada Internet; lo que, ha dado lugar a la creación de leyes de observancia en los distintos poderes de la unión. Ello, ha imperado en la innovación y perfeccionamiento de formas, métodos y medios de ejecución, dada la importancia que representa la utilización de los medios electrónicos y dicha red global; por lo que, se ha buscado su aprovechamiento en diversas áreas.

Enseguida, se expondrán algunos ejemplos de su aplicación, así como diversas disposiciones relativas a la utilización y ejecución de estos descubrimientos de la ciencia.



Fuente. enlace.vazquezchagoya.com

Figura 1-1. Sesión del Pleno de la H. Cámara de Diputados. (Fotografía vista en Internet el 20 de marzo de 2010).

En la Cámara de Diputados, se instaló un sistema electrónico de asistencia y votación, en agosto de 1998, el cual, dada la temporalidad de éste, y la reciente revisión que hizo el Instituto Politécnico Nacional, resultó incompatible con las nuevas tecnologías; por lo que, el Comité de Administración de dicha Cámara, autorizó la licitación para la adquisición e implementación de un nuevo sistema electrónico de votación de asistencia, audio y despliegue de información legislativa en el salón de sesiones de la H. Cámara de Diputados; que no dudo pronto se instalará en el recinto legislativo, no obstante la oposición al cambio.

Esta propuesta de los especialistas del Instituto Politécnico Nacional, va dirigida hacia un sistema de bio-verificación o bio-comprobación para emitir el voto con huella dactilar, que afirman expertos, mejoraría el desarrollo de las actividades parlamentarias en las Sesiones del Pleno de esta Cámara; además, de entrar a la modernidad de los Congresos de Canadá, Francia, Alemania o Inglaterra.

Otro ejemplo destacado, es el sistema utilizado en el Registro Nacional de Vehículos, (RENAVE), creado en la Ley del Registro Público Vehicular, publicada en la Sección Primera del Diario Oficial de la Federación, el 1 de septiembre de 2004;

la cual tiene por objeto establecer y regular la operación, funcionamiento y administración del Registro Público Vehicular. Dicho Registro es un instrumento de información del Sistema Nacional de Seguridad Pública, que tiene como propósito otorgar seguridad pública y jurídica a los actos que se realicen con vehículos. Se encuentra conformado por una base de datos integrada por la información que de cada vehículo proporcionan las autoridades federales, las Entidades Federativas y los sujetos obligados a realizar las inscripciones y a presentar los avisos, de conformidad con lo dispuesto en la citada ley.



Fuente. entretodos.com.mx

Figura 1-2. Página web de la Secretaría de Seguridad Pública. (Fotografía vista en Internet el 20 de marzo de 2010).

Para mantener actualizado el Registro, las autoridades federales y las de las Entidades Federativas, de conformidad con sus atribuciones, suministran la información relativa a altas, bajas, cambio de propietario, emplacamientos, infracciones, pérdidas, robos, recuperaciones, pago de tenencias y contribuciones,

destrucción de vehículos, gravámenes y otros datos con los que cuenten. Por su parte, el Secretariado Ejecutivo, mediante los instrumentos de información nacional sobre seguridad pública que correspondan, incorpora al Registro la información que le proporcionen las Procuradurías, relativa a robos, recuperaciones y destrucción de vehículos; ello, en observancia al artículo 6º, del ordenamiento legal en cita.

En esa tesitura, fue creada la página web del Sistema Nacional de Seguridad Pública, de la Secretaría de Seguridad Pública, quien en conjunto con la Procuraduría General de Justicia, quien proporciona a ésta información sobre reporte de robo de automóviles, despliega en su página información sobre la condición de los vehículos, reportando su robo o no, en su caso.

SISE

Sistema Integral de Seguimiento de Expedientes

[Expediente Electrónico](#) [Actuario](#) [Sentencias](#) [Tesis FESE](#) [Personal](#)
[Reportes estadísticos](#) [SiBAP](#) [Mis datos](#) [Sitios de interés](#) [Ayuda](#)

Fuente. Sistema Integral de Seguimiento de Expedientes.

Figura 1-3. Extracto de la página web del Sistema Integral de Seguimiento de Expedientes del Poder Judicial de la Federación.

Por otra parte, por Acuerdo General 28/2001 del Pleno del Consejo de la Judicatura Federal, publicado en el Diario Oficial de la Federación, el 25 de mayo de 2001, se estableció la obligatoriedad del uso del Sistema Integral de Seguimiento de Expedientes. Ello, fue considerado en virtud de que la Ley Orgánica del Poder Judicial de la Federación, en su artículo 81, fracción XXXV, confiere al Consejo de la Judicatura Federal la facultad de fijar las bases de la política informática y de información estadística que permitan conocer y planear el desarrollo del Poder Judicial de la Federación, con excepción de la Suprema Corte de Justicia de la Nación

y del Tribunal Electoral; ello, derivado de que una de las necesidades prioritarias de los órganos jurisdiccionales del Poder Judicial de la Federación, es contar con información completa, veraz, oportuna y uniforme para la adecuada toma de decisiones, de la que destaca la información estadística, en particular la proveniente de los propios órganos jurisdiccionales federales; estableciéndose así el siguiente acuerdo, mismo que se transcribe a continuación:

“ACUERDO

PRIMERO.- Establecimiento del Sistema Integral de Seguimiento de Expedientes.- Se establece el Sistema Integral de Seguimiento de Expedientes (SISE), como programa automatizado de captura y reporte de datos estadísticos sobre el movimiento de asuntos del conocimiento de los órganos jurisdiccionales del Poder Judicial de la Federación, con excepción de la Suprema Corte de Justicia de la Nación y del Tribunal Electoral.

SEGUNDO.- Empleo Obligatorio del Programa, Almacenamiento de los Datos y su Utilización.- Es obligación de los Titulares de Tribunales de Circuito y Juzgados de Distrito del Poder Judicial de la Federación el empleo del Sistema Integral de Seguimiento de Expedientes, para el registro de los movimientos de los juicios de amparo, procesos y recursos que ante ellos se tramiten; de igual manera, bajo la supervisión del secretario que al efecto designen dichos Titulares, deberá realizarse la captura diaria de datos que asegure la permanente actualización y veracidad de la información contenida en el Sistema.

La información obtenida de cada uno de los órganos obligados a operar el Sistema de referencia, podrá ser utilizada para efectos de control, gestión y administración interna, así como para responder a las consultas que de manera ordinaria o extraordinaria formulen los órganos competentes del Poder Judicial de la Federación.

Los datos que reporte el mencionado Sistema, serán concentrados en forma automatizada en los servidores centrales del Poder Judicial de la Federación ubicados en la Ciudad de México y en los servidores regionales que actualmente se tienen instalados en diversas ciudades de la República; y la información así almacenada se utilizará como apoyo en la toma de decisiones relativas al control, administración, vigilancia, disciplina y planeación del Poder Judicial de la Federación.

TERCERO.- Adecuación del Sistema.- Las características de la información requerida, así como la normatividad para registrar los datos que exige el Sistema, podrán adecuarse conforme lo determine la experiencia de su operación y los avances tecnológicos que aporten nuevas herramientas para facilitar y optimizar la extracción, concentración y explotación de la información disponible, para control interno de los Tribunales de Circuito y Juzgados de Distrito del Poder Judicial de la Federación y, en un aspecto general, por los órganos de gobierno del Consejo de la Judicatura Federal.

CUARTO.- Supervisión del Sistema.- La operación del Sistema Integral de Seguimiento de Expedientes será supervisada por el Grupo de Estadística Judicial, con el apoyo del personal especializado que se requiera.

QUINTO.- Participación de la Visitaduría Judicial en el Sistema Integral de Seguimiento de Expedientes.- La Visitaduría Judicial, con motivo de las visitas de inspección que realice a los órganos jurisdiccionales del Poder Judicial de la Federación, supervisará que el registro de expedientes en el Sistema se realice de manera diaria y que la información almacenada corresponda fielmente con lo actuado; en caso de omisión, será materia de recomendación, de la que se anexará copia al expediente personal del Titular que infrinja las disposiciones contenidas en este Acuerdo.

SEXTO.- Area Competente para la Solución de Problemas Técnicos.- La Dirección General de Informática del Consejo de la Judicatura Federal, es el área a la que corresponde solucionar los problemas técnicos que surjan con motivo de la operación del Sistema Integral de Seguimiento de Expedientes, de la red de comunicaciones y del equipo de cómputo destinado a la captura de datos y, en caso de estimar que se trata de un asunto que no es de su competencia, lo comunicará al Comité Consultivo Encargado de la Actualización y Supervisión del Sistema Integral de Seguimiento de Expedientes, con independencia de que promueva lo conducente, en el área respectiva, para resolverlo.

SEPTIMO.- Inicio de la Captura de Datos.- Los Titulares de los Tribunales de Circuito y Juzgados de Distrito del Poder Judicial de la Federación, ordenarán que la captura de los datos en el Sistema Integral de Seguimiento de Expedientes comprenda los movimientos de los expedientes a partir del dos de abril de dos mil uno.

TRANSITORIOS

PRIMERO.- El presente Acuerdo entrará en vigor el día de su aprobación.

SEGUNDO.- Publíquese este Acuerdo en el **Diario Oficial de la Federación** y en el Semanario Judicial de la Federación y su Gaceta.

EL LICENCIADO **GUILLERMO ANTONIO MUÑOZ JIMENEZ**, SECRETARIO EJECUTIVO DEL PLENO DEL CONSEJO DE LA JUDICATURA FEDERAL, CERTIFICA: Que este Acuerdo General 28/2001, del Pleno del Consejo de la Judicatura Federal, Que Establece la Obligatoriedad del Uso del Sistema Integral de Seguimiento de Expedientes, fue aprobado por el propio Pleno, en sesión de dieciséis de mayo de dos mil uno, por unanimidad de votos de los señores Consejeros: Presidente Ministro **Genaro David Góngora Pimentel**, **Adolfo O. Aragón Mendía**, **Manuel Barquín Alvarez**, **Enrique Sánchez Bringas** y **José Guadalupe Torres Morales**.- México, Distrito Federal, a dieciséis de mayo de dos mil uno.- Conste.- Rúbrica.”.

En ese sentido, opera el Sistema Integral de Seguimiento de Expedientes (SISE), como programa automatizado de captura y reporte de datos estadísticos sobre el movimiento de asuntos del conocimiento de los órganos jurisdiccionales del Poder Judicial de la Federación, con excepción de la Suprema Corte de Justicia de la Nación y del Tribunal Electoral.

Fue así, como mediante Acuerdo General 21/2007, publicado en el Diario Oficial de la Federación, el 7 de julio de 2007, se sentaron las bases para la creación del expediente digital o electrónico, así como la firma electrónica.

EXPEDIENTE ELECTRÓNICO

Amparo Indirecto

Selección de Cuaderno

Principal (Haga clic sobre la imagen)



Incidental (Haga clic sobre la imagen)



Fuente. Sistema Integral de Seguimiento de Expedientes

Figura 1-4. Extracto de la página web del Sistema Integral de Seguimiento de Expedientes del Poder Judicial de la Federación.

En el citado Acuerdo General 21/2007, se consideró de manera destacada, lo que se reproduce a continuación:

“**QUINTO.-** La incorporación del uso de recursos tecnológicos ha facilitado la comunicación y seguimiento de los asuntos, tanto por los órganos jurisdiccionales como por los justiciables, lo que ha permitido un ágil manejo de la información, al regular la captura de datos en forma electrónica en un sistema que puede consultarse en la

página de *Internet* del Consejo, a través del que se difunden las listas de síntesis de acuerdos de los diversos tipos de asuntos del conocimiento de los tribunales de Circuito y juzgados de Distrito y permite a los interesados en los juicios, enterarse de manera rápida y sencilla de la existencia de las determinaciones judiciales, de acuerdo a las disposiciones legales respectivas;

SEXTO.- Actualmente, los servidores públicos del Poder Judicial de la Federación, de acuerdo a sus facultades, tienen acceso al sistema, mediante una clave para capturar y consultar los datos de los acuerdos y resoluciones dictadas por los órganos jurisdiccionales federales en los asuntos de su competencia y envían con la firma electrónica de los titulares los reportes estadísticos;

SEPTIMO.- Los avances tecnológicos han permitido al Consejo de la Judicatura Federal contar con el medio electrónico donde se incluye la configuración del expediente virtual, es decir, una copia digitalizada de las constancias de los autos del expediente real y el uso de una firma electrónica para todos los que intervienen en los procedimientos judiciales.

Este medio de comunicación puede aprovecharse para enviar y recibir todo tipo de comunicaciones, promociones y documentos que se almacenarán para consulta y acuerdo en los procedimientos jurisdiccionales que establecen las leyes de la materia de que se trate, expidiéndose constancias de recibo y entrega;

OCTAVO.- El medio electrónico en comento contendrá toda la información de los expedientes en los juicios que conocen los órganos jurisdiccionales, de manera que las partes, los terceros interesados, los auxiliares de la administración de justicia o personas autorizadas por los órganos jurisdiccionales puedan consultar en forma inmediata lo que legalmente les corresponda;

NOVENO.- Las determinaciones de los órganos jurisdiccionales del Poder Judicial de la Federación, con excepción de la Suprema Corte de Justicia de la Nación y del Tribunal Electoral, se hacen del conocimiento de las partes con fundamento en las leyes que regulan las notificaciones en los procedimientos judiciales, como son, entre otras, la Ley de Amparo en sus artículos 28, fracción III, último párrafo, 29, fracción II y 30; el Código Federal de Procedimientos Penales en su artículo 107; la Ley Federal de Concursos Mercantiles en su artículo 133; el Código de Comercio en su artículo 1068, fracciones II y III; y el Código Federal de Procedimientos Civiles en sus artículos 316 y 320 .

De conformidad con lo dispuesto en el último precepto legal citado, si alguna parte dentro del procedimiento se manifiesta ante el órgano jurisdiccional sabedora de la providencia, la notificación no realizada conforme a las disposiciones legales, surtirá sus efectos como si estuviese hecha con arreglo a la ley;

DECIMO.- Para que las partes, los terceros interesados, los auxiliares de la administración de justicia o personas autorizadas por los órganos jurisdiccionales tengan acceso al expediente electrónico de su interés contenido en el sistema, es necesario que estén autorizadas por el órgano jurisdiccional con una Clave Personal que se denominará Firma Electrónica para el Seguimiento de Expedientes (FESE) y que producirá los mismos efectos jurídicos que la firma autógrafa.

La Clave Personal se proporcionará por los órganos jurisdiccionales, previo llenado del formato que estará a disposición del interesado en el portal del Consejo de la Judicatura Federal y que se imprimirá en dos tantos, para presentarse acompañado de original y copia de su identificación oficial y/o personal (credencial expedida por el Instituto Federal Electoral o pasaporte) y constancia de domicilio en la oficialía de partes de éstos, para que el secretario autorizado coteje las firmas, certifique las copias, devuelva los originales y tome razón de recibo de la clave, documentos que deberá resguardar bajo su responsabilidad.

El formato incluirá la protesta de decir verdad de que los datos asentados en el mismo son ciertos y que pueden verificarse, bajo la pena de incurrir en el delito de falsedad de declaraciones dadas a una autoridad judicial en caso de ser falsos, así como su aceptación de que la clave otorgada es intransferible, que el uso de ésta es de su exclusiva responsabilidad y, por considerarse una firma electrónica avanzada, debe equipararse a su firma estampada en original.

El formato contendrá la manifestación de voluntad de que al usar su clave como Firma Electrónica para el Seguimiento de Expedientes (FESE) para ingresar al sistema y abrir los archivos que contengan acuerdos o resoluciones, se hace sabedor de éstos en la fecha y hora que lo haga, independientemente del día en que se fijen las listas con las publicaciones en los estrados o los rotulones en las puertas de los tribunales de Circuito y juzgados de Distrito, según corresponda;

DECIMOPRIMERO.- A las personas con clave o Firma Electrónica para el Seguimiento de Expedientes (FESE), se les permitirá el acceso al sistema para la consulta de promociones que legalmente les correspondan, documentos, acuerdos y resoluciones contenidos en el expediente de su interés. El sistema emitirá una constancia electrónica de la consulta realizada que acreditará que el usuario se hizo sabedor de la determinación judicial, la que se imprimirá en el órgano jurisdiccional y se agregará para constancia en autos.

De requerir copia certificada de los documentos consultados, el usuario, vía electrónica, los imprimirá y ocurrirá al órgano jurisdiccional correspondiente para su compulsión y certificación.

El escrito de petición de compulsión y certificación se agregará con el acuerdo de autorización y la razón de recibo al expediente, con lo que se dará cumplimiento a lo dispuesto en las leyes de la materia, evitando impresiones en el órgano jurisdiccional, de documentos, acuerdos, testimonios de resoluciones o sentencias, así como tardanza por fotocopiado y, consecuentemente, en la entrega de las certificaciones;

DECIMOSEGUNDO.- Los titulares de los órganos jurisdiccionales serán los responsables de vigilar la digitalización de las promociones y documentos que presenten las partes y se agreguen oportunamente los acuerdos, resoluciones o sentencias y toda la información relacionada con los expedientes en el sistema, una vez que se instale el equipo y entre en operación el programa informático en los órganos jurisdiccionales, lo que se hará en la medida que el presupuesto del Consejo de la Judicatura Federal lo permita.

Corresponderá a la Comisión de Administración del Consejo de la Judicatura Federal, establecer la normatividad y los mecanismos de aplicación informática necesarios para controlar el flujo de información, así como la definición de una unidad para el control de certificación de firmas; la expedición de la clave personal de la Firma Electrónica para el Seguimiento de Expedientes (FESE), establecerá las modalidades de acceso y consulta de la información, según la secrecía que establezcan los ordenamientos legales y para la seguridad del almacenamiento de la información.”.

En consecuencia, con fundamento en las disposiciones constitucionales y legales señaladas, y por las razones expuestas, se expide el siguiente

ACUERDO

PRIMERO.- Se establece ante los órganos jurisdiccionales la utilización por las partes o personas autorizadas, la Firma Electrónica para el Seguimiento de Expedientes (FESE) para todos aquéllos trámites señalados en este Acuerdo.

Para la utilización de la Firma Electrónica para el seguimiento de expedientes el Consejo implementará en los órganos jurisdiccionales, los sistemas que permitan la digitalización de las constancias que obren en los expedientes del conocimiento de los tribunales de Circuito y juzgados de Distrito.

SEGUNDO.- Se instituye la clave personal o Firma Electrónica para el Seguimiento de Expedientes (FESE), como medio controlado de ingreso al sistema para consultar, enviar y recibir promociones, documentos, acuerdos, resoluciones, sentencias y comunicaciones oficiales relacionadas con los asuntos competencia de los órganos jurisdiccionales, la que será otorgada y certificada por éstos, concentrada y controlada por la Unidad para el Control de Certificación de Firmas.

TERCERO.- Se autoriza el acceso al sistema de expediente electrónico a las partes, los terceros interesados, los auxiliares de la administración de justicia o personas autorizadas por los órganos jurisdiccionales, a la información del expediente de su interés.

CUARTO.- Las partes en los juicios, terceros interesados, auxiliares de la administración de justicia o personas autorizadas por los órganos jurisdiccionales que soliciten la asignación de la Firma Electrónica para el Seguimiento de Expedientes (FESE) y realicen la consulta respectiva, aceptan que se les tendrá como sabedoras del contenido de los acuerdos o resoluciones, promociones que legalmente les correspondan, informes previos y justificados, pruebas, dictámenes, inspecciones, diligencias y toda clase de documentos e información relativa al asunto, donde sean partes o estén autorizados por el órgano jurisdiccional, siempre que obren digitalizados en el sistema.

QUINTO.- Los servidores públicos adscritos a los órganos jurisdiccionales podrán, entre sí, y para con las personas con Firma Electrónica para el Seguimiento de Expedientes (FESE), y de éstas para con aquéllos, utilizar el sistema electrónico para remitir y recibir comunicaciones oficiales, promociones y documentos digitalizados relacionados con los expedientes de procedimientos judiciales.

SEXTO.- Los titulares de los órganos jurisdiccionales serán responsables de vigilar que se digitalicen e incorporen en el sistema electrónico las promociones y documentos que presenten las partes, y que se agreguen oportunamente los acuerdos, resoluciones, sentencias o cualquier determinación que emitan relacionada con los asuntos de su competencia, una vez que se instale el equipo y entre en operación el programa informático.

SEPTIMO.- La Comisión de Administración del Consejo de la Judicatura Federal determinará y formará los mecanismos de aplicación informática necesarios para controlar el flujo de información; creará la Unidad para el Control de Certificación de Firmas, determinará la clave personal de la Firma Electrónica para el Seguimiento de Expedientes (FESE), y establecerá las modalidades de la información que se remita y consulte con esas claves.

TRANSITORIOS

PRIMERO.- El presente acuerdo entrará en vigor el día de su aprobación.

SEGUNDO.- La aplicación de este sistema electrónico en los órganos jurisdiccionales se implementará paulatinamente conforme a las posibilidades presupuestales que permita la adquisición y dotación del equipo y programas de cómputo.

TERCERO.- En tanto se crea la Unidad para el Control de Certificación de Firmas, la función de concentración y control será realizada por la Dirección General de Estadística y Planeación Judicial del Consejo de la Judicatura Federal.

CUARTO.- Publíquese este acuerdo en el Diario Oficial de la Federación, así como en el Semanario Judicial de la Federación y su Gaceta.

El LICENCIADO **GONZALO MOCTEZUMA BARRAGAN**, SECRETARIO EJECUTIVO DEL PLENO DEL CONSEJO DE LA JUDICATURA FEDERAL, CERTIFICA: Que este Acuerdo General 21/2007, del Pleno del Consejo de la Judicatura Federal, que Establece la Firma Electrónica para el Seguimiento de Expedientes (FESE), fue aprobado por el Pleno del propio Consejo, en sesión ordinaria de veintitrés de mayo de dos mil siete, por unanimidad de votos de los señores Consejeros: Presidente Ministro Guillermo I. Ortiz Mayagoitia, Luis María Aguilar Morales, Elvia Díaz de León D'Hers, María Teresa Herrera Tello y Miguel A. Quirós Pérez.- México, Distrito Federal, a veintitrés de mayo de dos mil siete.- Conste.- Rúbrica.”.

Dicho Acuerdo General 21/2007, es concordante con los Acuerdos Generales Conjuntos 1/2009, 2/2009 y 3/2009, de los Plenos de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal, relativos a la transferencia, digitalización, depuración y destrucción de los expedientes generados en los Juzgados de Distrito y Tribunales Unitarios y Colegiados de Circuito; en los cuales cabe destacar el Capítulo Cuarto, relativo a la digitalización de las actuaciones judiciales; cuyo tenor es el siguiente:

“CAPITULO CUARTO

DE LA DIGITALIZACION DE LAS ACTUACIONES JUDICIALES

DECIMO QUINTO. En relación con los expedientes bajo resguardo de la Suprema Corte al momento en que entre en vigor este Acuerdo General Conjunto, Informática llevará a cabo su digitalización, de conformidad con la relación que el Centro de Documentación y Análisis le entregue, en la que precisen los casos en que se digitalizará la demanda y la sentencia relativas a los asuntos en los que se haya negado o concedido el amparo directo; en la inteligencia de que deberá remitir una versión a la Dirección General de Planeación de lo Jurídico de la Suprema Corte para el análisis estadístico que corresponda.

En los casos excepcionales que apruebe el Comité, o el órgano de la Suprema Corte que éste determine, se digitalizará total o parcialmente algún expediente, atendiendo a su estado de conservación, a la estadística de consultas que registren y, en particular, a su relevancia documental.

DECIMO SEXTO. Informática llevará a cabo las acciones necesarias para que la información digitalizada por la Suprema Corte relativa al archivo judicial bajo su resguardo se pueda difundir y consultar en Internet de manera ágil; y para efectos de su preservación, determinará las características de los archivos electrónicos que se generen. Para ello, se coordinará con el Centro de Documentación y Análisis.

DECIMO SEPTIMO. En el caso de los expedientes diversos de los señalados en el punto Décimo Quinto de este Acuerdo General Conjunto, los Tribunales Colegiados de Circuito llevarán a cabo la digitalización de las actuaciones que ameriten ese tratamiento a fin de conservar y difundir su contenido, una vez que inicien el registro de firma electrónica, de conformidad con lo establecido en el Acuerdo General 21/2007 del Pleno del Consejo de la Judicatura Federal, que establece la Firma Electrónica para el seguimiento de expedientes (FESE), publicado en el Diario Oficial de la Federación el siete de junio de dos mil siete.

DECIMO OCTAVO. Los Tribunales Colegiados de Circuito, al transferir físicamente los expedientes de archivo reciente con más de tres años de haberse ordenado su archivo, a los depósitos de la Suprema Corte, deberán dar aviso a Estadística y Planeación, mediante oficio, para que ésta transfiera en formato digital al programa que administra la Suprema Corte, todas las actuaciones judiciales que integran un asunto y se encuentren digitalizadas.

DECIMO NOVENO. Estadística y Planeación se coordinará con el Centro de Documentación y Análisis y con Informática para establecer un protocolo de intercambio de información entre el programa que administra relativo a la digitalización de actuaciones en los Tribunales Colegiados de Circuito y el programa que administra la Suprema Corte para el aprovechamiento de la información digital transferida por el Consejo.”.

Así, nace el expediente electrónico judicial cuya página web cuenta con un panel central de consulta, en el cual se puede visualizar la fecha del acuerdo, la publicación, la promoción, el contenido de la determinación judicial, el tipo de determinación judicial, el acuse de la determinación judicial, y la notificación o constancia de conocimiento, en juicios de amparo indirecto, causas penales, procesos civiles o administrativos, medidas precautorias, procedimiento de extradición, comunicaciones oficiales enviadas o recibidas (exhortos, rogatorias, despachos), y concursos mercantiles.

Cabe mencionar, la colaboración que tuvo la Universidad Nacional Autónoma de México, quien dio un diagnóstico sobre el Programa de Digitalización de Expedientes Judiciales, en el cual nuestra Máxima Casa de Estudios, señaló que actualmente la digitalización es el proceso idóneo para la conservación y difusión de los expedientes judiciales, y por cuanto hace a las gestiones a llevar a cabo para su continuidad; y, en esencia, recomendó diseñar y desarrollar un programa permanente que permita digitalizar los expedientes judiciales tanto en el Máximo Tribunal como en los Tribunales de Circuito y Juzgados de Distrito; así como otro programa que permita digitalizar el acervo generado por la Suprema Corte y dichos órganos jurisdiccionales federales que se encuentra actualmente bajo resguardo del más Alto Tribunal a través del Centro de Documentación y Análisis; aunado a ello, se precisó la importancia de que se contemple la posibilidad de digitalizar no sólo la sentencia sino todo el expediente, cuando éste tenga valor histórico; situación que actualmente ya acontece.

Asimismo, cabe destacar la consulta de criterios jurisprudenciales que se puede realizar a través del sistema Jurisprudencia y Tesis Aisladas IUS, que es un instrumento óptico que contiene alrededor de 222,000 tesis jurisprudenciales y aisladas del Pleno y Salas de la Suprema Corte y de los Tribunales Colegiados de Circuito, publicadas en el Semanario desde junio de 1917; asimismo 28,304 criterios integrados en los diferentes Apéndices al propio Semanario desde 1954 -con sus actualizaciones correspondientes-, y 6,974 más, incluidos en algunos informes de labores; así como el Sistema Computarizado para el Registro Único de Profesionales del Derecho, ante los Tribunales de Circuito y Juzgados de Distrito, emanado del Acuerdo General 24/2005, del Pleno del Consejo de la Judicatura Federal, publicado en el Diario Oficial de la Federación de 18 de julio de 2009; que consiste en una base de datos con información clasificada como confidencial, de uso interno en todos los órganos jurisdiccionales y del área responsable del Consejo de la Judicatura Federal, y, en el cual se ingresan a través de una solicitud de registro, los datos de la cédula profesional, o de la copia certificada de ésta, según sea el caso,

Por otro lado, dentro de las funciones que desarrolla el **Registro Civil del Distrito Federal**, como la certificación de los testimonios de las actas relativas a nacimiento, reconocimiento de hijos, adopción, matrimonio, etcétera; actualmente pueden autenticarse con firma autógrafa o electrónica; ello, en atención a las diversas reformas al Código Civil para el Distrito Federal, publicadas en la Gaceta Oficial, el 13 de enero de 2004; entre ellas, las reformas al artículo 48 de dicho dispositivo legal, el cual, se transcribe a continuación:

“Artículo 48. Toda persona puede pedir testimonios completos o en extracto de las actas del Registro Civil; así como de los apuntes y documentos con ellas relacionadas y los jueces y registradores estarán obligados a darlos.- - - La certificación de los testimonios de las actas del Registro Civil podrá autenticarse con firma autógrafa o electrónica. Por firma electrónica se entenderá la firma, clave, código o cualquier otra forma de autenticar por medios electrónicos, la autorización del funcionario competente según el sistema que instrumente el titular del Registro Civil conforme a lo que disponga el reglamento respectivo.- - - Las copias

certificadas y las certificaciones emitidas por los servidores públicos facultados para ello y que sean autenticadas a través de firma electrónica, tendrán el mismo valor jurídico y probatorio que las suscritas en forma autógrafa.”

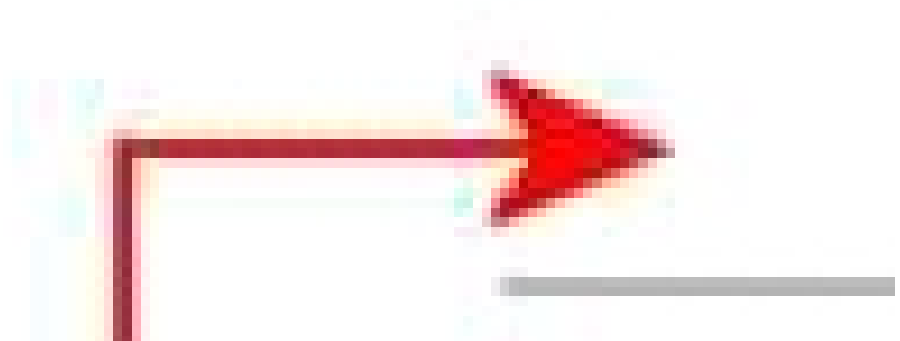
Con ello, se agiliza la función de dicha Institución en lo que refiere a la expedición de actas, dando así certeza probatoria de los documentos que expida dicha institución bajo una firma electrónica.

En materia tributaria, la Secretaría de Finanzas del Gobierno del Distrito Federal, derivado de los propósitos fundamentales que es la de promover, fomentar y facilitar el cumplimiento de las obligaciones fiscales de los contribuyentes, el 26 de marzo de 2002, se publicaron en la Gaceta Oficial del Distrito Federal, las “Reglas de carácter general para la recepción y control de pagos que se efectúan a través de instituciones de crédito, mediante el sistema de cargos automáticos, por Internet o directamente en ventanilla bancaria”, a las que se adjunto el Formato Universal de la Tesorería 2002, para el pago de diversos conceptos autorizados.

Luego, se publica el Acuerdo por el que se aprueba la forma oficial denominada “Formato Universal de la Tesorería”, sustituyendo al primer formato; ello, con fundamento en el Código Financiero del Distrito Federal; el cual, en sus artículos 30 y 125, fracción III, establecen, respectivamente, que los contribuyentes tendrán la obligación de presentar declaraciones para el pago de las contribuciones en los casos que así lo señala dicho ordenamiento; correspondiendo a las autoridades fiscales elaborar formularios de declaración que puedan ser llenados fácilmente por los contribuyentes, y distribuirlos con oportunidad.

Este formato se encuentra en la página web del Gobierno del Distrito Federal, Secretaría de Fianzas, en la cual el contribuyente puede acceder, y obtener las formas oficiales, con las cuales puede realizar el pago de 81 diferentes conceptos entre impuestos, trámites y multas. Es llenado electrónicamente (nombre, denominación o razón social según se trate, domicilio, concepto o clave de pago), e impreso para su presentación en Bancos y Tiendas de Autoservicio, para su pago. Los conceptos que

se pueden pagar a través de este formato, por citar algunos, son: licencias, trámites vehiculares y permisos, multas vehiculares, copias certificadas, e inscripción de actos ocurridos en el extranjero o fuera del Distrito Federal.



Fuente. finanzas.df.gob.mx

Figura 1-5. Formato Universal de Tesorería. (Fotografía vista en Internet el 20 de marzo de 2010).

En materia de iniciación de averiguaciones previas, el 28 de agosto de 2008, la Asamblea Legislativa del Distrito Federal, reformó los artículos 9 bis y 276, del Código de Procedimientos Penales para el Distrito Federal, que obliga al Ministerio Público a recibir la declaración escrita o verbal por cualquier delito, o vía portal electrónico de la Procuraduría General de la República, únicamente por los delitos que se persiguen por querrela y no sean considerados como graves.

Fuente. df-gob.mx

Figura 1.6. Ministerio Público Virtual. (Fotografía vista en Internet el 20 de marzo de 2010).

El procedimiento es el siguiente: i). identificar si el caso procede vía Internet; ii). llenar y enviar el formato en línea; iii). ingresar los datos de denunciante/querellante en el sistema; si se desea puede adjuntarse la declaración por escrito en formato PDF, con la firma e identificación oficial digitalizados del denunciante/querellante; iv). si el trámite es para una acta especial, el sistema asignará un folio y con el mismo el denunciante/querellante puede acudir a la Fiscalía de la Delegación que elija éste; v). si el trámite es para iniciar una averiguación previa, la Dirección de la Unidad de Recepción por Internet (DUR), enviará al denunciante/querellante, un correo electrónico asignándole una cita en la Fiscalía correspondiente; vi). si el denunciante/querellante no asiste a la cita, su trámite se tendrá por no efectuado, quedando a salvo sus derechos para volver a iniciar por esta vía o en la agencia del Ministerio Público; y, vii). se recomienda estar al pendiente de la recepción del correo electrónico.

Por su parte, la Presidencia de la República, las Secretarías de Estado, los Departamentos Administrativos y la Consejería Jurídica del Ejecutivo Federal, que integran la Administración Pública Centralizada, así como los organismos descentralizados, las empresas de participación estatal, las instituciones nacionales de crédito, las organizaciones auxiliares nacionales de crédito, las instituciones nacionales de seguros y de fianzas y los fideicomisos, que componen la administración pública paraestatal, así como la mayoría de los órganos desconcentrados con que cuentan las Secretarías de Estado y los Departamentos Administrativos; cuentan con página web fácilmente localizadas a través de los buscadores, y con diseños de alto impacto; en los cuales resaltan los links relativos a su historia, servicios, mapa de sitio, actividades, leyes y reglamentos, información, asesoría, comunicados, encuestas, contacto, noticias, etcétera.



Fuente. cdn.alt1040.com

Figura 1.7. Página web de la Presidencia de la República. (Fotografía vista en Internet el 20 de marzo de 2010).



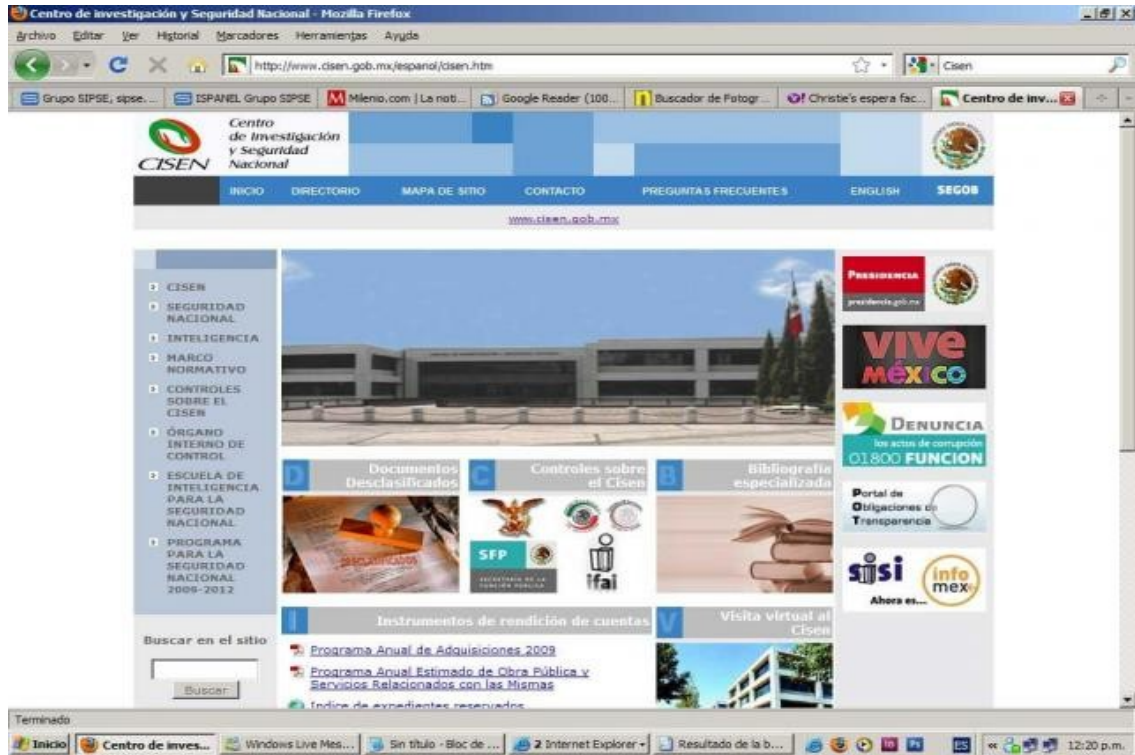
Fuente. technosat.wordpress.com

Figura 1.8. Página web de la Secretaría de la Defensa Nacional. (Fotografía vista en Internet el 20 de marzo de 2010).



Fuente. technosat.wordpress.com

Figura 1.9. Página web de la Secretaría de Hacienda y Crédito Público. (Fotografía vista en Internet el 23 de marzo de 2010).



Fuente. extraprimera.blogspot.com

Figura 1.10. Página web de la Secretaría de Gobernación. (Fotografía vista en Internet el 24 de marzo de 2010).

Profecco

Fuente. matuk.com

Figura 1.11. Página web de la Secretaría de Economía. (Fotografía vista en Internet el 20 de marzo de 2010).

The image shows a screenshot of the INAPAM website with 11 numbered callouts pointing to specific features:

- 1:** Logo of INAPAM (Instituto Nacional de las Personas Adultas Mayores).
- 2:** Navigation menu items: Inicio, Mapa del Sitio, Contacto, English, SEDESOL.
- 3:** Mexican coat of arms logo.
- 4:** Main banner image showing a man speaking at a podium with the SEDESOL logo.
- 5:** Search bar with a 'Buscar' button.
- 6:** 'ENLACES' section listing various links like 'Congresos, Foros y Convocatorias'.
- 7:** 'TEMAS DE INTERÉS' sidebar with a list of topics and a 'ver más' link.
- 8:** News article titled 'Designan a Alejandro Lucas Orozco Rubio titular de Inapam'.
- 9:** 'CONVENIOS INAPAM' section with the headline '¡Aprovecha los descuentos!'.
- 10:** 'DENUNCIA' section with the text 'los actos de corrupción' and '01800 FUNCION'.
- 11:** Footer area containing contact information and 'Visitas a la sección: 4053'.

Fuente. www.inapam.gob.mx

Figura 1.12. Página web de la Secretaría de Desarrollo Social. (Fotografía vista en 2010).

Asimismo, diversas dependencias de carácter social, educativo y económicas, se han sumado a la creación de sus páginas web, resultando mayor la penetración de la ciudadanía en las diversas ramas; ello, a través de la comunicación y facilitación de la búsqueda de información; lo que, ha llevado a la actualización constante del aprendizaje.

En ese panorama, se encuentran los siguientes ordenamientos en cuyos textos se hace referencia a Internet, entre otros, a saber: Código Federal de Instituciones y Procedimientos Electorales; Código Federal de Procedimientos Penales; Código Fiscal de la Federación; Estatuto del Servicio Fiscalizador de Carrera de la Auditoría Superior de la Federación; Estatuto del Servicio Profesional en el Instituto Federal de Acceso a la Información Pública; Estatuto Orgánico de Aeropuertos y Servicios Auxiliares; Estatuto Orgánico de la Comisión Nacional de Cultura Física y Deporte; Estatuto Orgánico de la Comisión Nacional Forestal; Estatuto Orgánico de la Procuraduría Federal del Consumidor; Ley de Coordinación Fiscal; Ley de Fiscalización y Rendición de Cuentas de la Federación; Ley de Instituciones de Crédito; Ley de la Policía Federal; Ley de Obras Públicas y Servicios Relacionados con las Mismas; Ley de Petróleos Mexicanos; Ley del Mercado de Valores; Ley del Servicio de Administración Tributaria; Ley Federal de Extinción de Dominio, Reglamentaria del Artículo 22 de la Constitución Política de los Estados Unidos Mexicanos; Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; Ley General de Bienes Nacionales; Ley de Educación del Distrito Federal; y, la Ley para Prevenir y Erradicar la Trata de Personas, el Abuso Sexual y la Explotación Sexual Comercial Infantil para el Distrito Federal.

De la misma manera, cabe mencionar la Ley Federal de Procedimiento Contencioso Administrativo, en cuyo ordenamiento ya se regula el juicio en línea, mismo que se encuentra en el Capítulo X, titulado “Del Juicio en Línea”, adicionado el 12 de junio de 2009; en cuyo artículo 58-A, y demás relativos, se establece que el juicio contencioso administrativo federal se promoverá, substanciará y resolverá en

línea, a través del Sistema de Justicia en Línea, establecido y desarrollado por el Tribunal Federal de Justicia Fiscal y Administrativa.

En esta nueva forma de impartición de justicia, pronto por aplicarse en agosto de 2011, se regula que el demandante señale expresamente su dirección de correo electrónico; se integre un expediente electrónico; se desahogue las pruebas testimoniales utilizando el método de videoconferencia; la firma electrónica avanzada, clave de acceso y contraseña sean proporcionadas a través del Sistema de Justicia en Línea del Tribunal; se emita el acuse de recibo electrónico una vez recibida por vía electrónica cualquier promoción de las partes; se realicen las notificaciones personales de las actuaciones y resoluciones, mediante correo certificado con acuse de recibo, o por oficio, a través del Sistema de Justicia en Línea del Tribunal, en donde el actuario debe elaborar la minuta electrónica en la que precise la actuación o resolución a notificar, así como los documentos que se adjunten a la misma; son hábiles las 24 horas de los días en que se encuentren abiertas al público las Oficinas de las Salas del Tribunal; y, demás actividades jurisdiccionales que se concluye, representan un avance en la llamada ciberjusticia.

1.4. Medios de comunicación.

Como medios de comunicación dentro del comercio electrónico se encuentran las vías de transmisión basadas en técnicas electrónicas, como la comunicación por medio del intercambio de datos electrónico (EDI).

El EDI comprende tres tipos de transmisión: la transmisión de datos de una terminal informática a otra utilizando un formato normalizado; la transmisión de mensajes electrónicos mediante el uso de normas patentadas o normas libres de acceso; y, la transmisión por vía electrónica de textos de formato libre, a través de Internet (correo electrónico), el télex, la telecopia o el fax.

La realización de operaciones a través de Internet, fundamentalmente por EDI,

el Web, correo electrónico y fax, han crecido de manera exponencial en los últimos años.⁷¹

1.5. Medios electrónicos.

Dada la evolución tecnológica, se ha estimado que no es viable considerar una lista de los medios electrónicos; sin embargo, se citan algunos ejemplos que han impactado en la sociedad, y han sido considerados importantes dentro del desarrollo comercial; considerados también con tal carácter dentro de la Ley Modelo de la CNUDMI Sobre Comercio Electrónico, a saber:

1.5.1. Internet.

Internet es una federación de redes. Es una infraestructura compartida constituida por protocolos que enlaza computadoras por todo el mundo, a través de mecanismos y protocolos, que permiten conectar usuarios entre sí, por medio de proveedores de servicios.⁷²

Cumple dos funciones básicas: medio de comunicación y medio de información. La primera la realiza a través del correo electrónico, foros de discusión y el servicio de llamadas telefónicas. Como medio de información, Internet es el centro de documentación más grande y completo del mundo.⁷³

Como antecedentes de Internet, se tiene que en los años sesenta, con el establecimiento de los llamados “canales de paquetes autónomos de información” – llamado así paquete autónomo, aquel método para fragmentar mensajes en subpartes llamadas paquetes y enviando dichos paquetes de información a su destinatario para que los reensamblara-, permitía que varios usuarios pudieran al mismo tiempo compartir la misma conexión en pequeñas unidades enviadas separadamente.

⁷¹ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob cit, pág. 26.

⁷² Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, pág. 62.

⁷³ Cfr. Rojas Amandi, Víctor Manuel, *El uso de Internet en el derecho*, Oxford University Press México, Sociedad Anónima de Capital Variable, Primera edición México, 2001, pág. 1.

En 1968, en los Estados Unidos fue desarrollada esta tecnología; sin embargo, no fue sino hasta 1970, que fue utilizada en la guerra fría, por la ARPA (Advanced Research Projects Agency o Agencia de Investigación de Proyectos Avanzados), quien inició el diseño de una red de computadoras como canal de comunicación, para efecto de que todas las bases estuvieran en posibilidad de comunicarse entre ellas y con el centro de control, en caso de destrucción de sus redes de comunicación, además de que debía reunir cualidades como: redundante, descentralizada y fácil de implementar. Redundante, en virtud de que la información debía encontrar más de una ruta desde su origen hasta su destino; descentralizada, pues no debía existir solo un centro que fuera fácil de eliminar; y, fácil de implementar al usarse la infraestructura existente.

Fue así como se crea ARPAnet, quien abrió su utilización a universidades, centros de investigación, dependencias de gobierno, instituciones extranjeras. Contaba con un número pequeño de máquinas, accesadas principalmente por usuarios académicos e investigadores, quienes de manera exponencial comenzaron a usar esta red, hasta que diseñadores de Estados Unidos, Inglaterra y Suecia, pusieron en marcha el protocolo IP en todo tipo de computadoras.

En virtud de que esta red había sido diseñada para utilizarla con diversos equipos, organizaciones comenzaron a emplear los equipos que tenían disponibles; ello, aunado a la evolución de la informática alrededor del año de 1983, que dio origen a las primeras computadoras personales, las cuales podían ser conectadas entre sí para formar redes de área local y de área extendida. En estos primeros inicios, la red se utilizaba especialmente para recibir y enviar correo electrónico.

Se comenzaron a construir redes de PC y estaciones de trabajo que utilizaban los protocolos IP de ARPAnet para comunicarse internamente, las cuales se multiplicaron mostrando lo positivo que sería que estas redes fueran dispersadas, conectadas entre sí. Sin embargo, al ponerse en práctica como lo fue NSFNET, en diversas universidades importantes a finales de 1980, trajo costos elevados, por lo que

NSF resolvió interconectar estos centros de cómputo mediante la tecnología IP de ARPAnet con líneas telefónicas, así para evitar grandes costos de las telecomunicaciones telefónicas de larga distancia, NSF diseñó un sistema que permitía a los centros de supercómputo conectarse con sus vecinos más cercanos para retransmitir la información; lo que resultó un éxito, pues al disminuir los costos del uso de la red, empezó a ser más accesible a otras universidades, y así a todo el mundo.

Seguido, en 1987, fue pasado el contrato de administración y mantenimiento de la red a Merit Network, Inc., en colaboración con MCI e IBM; y, en 1993 un joven científico Tim Berners-Lee, que trabajaba en el Laboratorio Europeo de Física de Partículas en Suiza (CERN), diseñó un sistema de hipertexto que permitía a usuarios de redes IP, navegar a través de una serie de documentos con despliegue de imágenes mediante la activación de enlaces en los documentos.

Así nace la WWW (World Wide Web), que es un conjunto de servicios basados en hipermedios, que refiere a la información que puede presentarse con distintos medios, accesibles a través de Internet, sin que exista un centro que administre esta red de información, pues está constituida por muchos servicios distintos que se conectan entre sí a través de referencias en los distintos documentos.

74

1.5.2. Télex.

Es un acrónimo de TELEprinter EXchange (intercambio entre teleimpresores). Es un servicio transmisor de mensajes mecanografiados mediante teletipos (telégrafos), que realizan directamente la transmisión de señales por teclado y la recepción en caracteres tipográficos. Este medio electrónico consta de un transmisor, un receptor y una central dotada de una computadora.⁷⁵

⁷⁴ Cfr. Téllez Valdés, Julio, ob cit, págs. 99-101.

⁷⁵ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, págs. 57-58.

1.5.3. Telégrafo.

El telégrafo es un conjunto de aparatos que sirven para transmitir despachos, o mensajes a larga distancia. Es un medio o tecnología similar a la utilizada en los medios electrónicos y ópticos, puesto que sirve para transmitir mensajes a larga distancia mediante impulsos eléctricos que circulan por un hilo metálico u óptico, o a través del viento en el caso de los inalámbricos.

El telégrafo permitía a las personas comunicarse y hacer pedidos de mercancías por medio de documentos breves, aun cuando no aparecían firmados por su autor. El uso frecuente de abreviaturas en las operaciones de compra y venta de mercancías por telegrama motivó la acuñación y el reconocimiento de los términos de comercio internacional por parte de la Cámara Internacional de Comercio, llamados *Incoterms*. Más adelante la comunicación a distancia se dio a través de la transmisión de mensajes telegrafados a través de teletipos.

La Ley Modelo sobre Comercio Electrónico, señala que los telegramas al ser información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, se consideran mensajes de datos; por lo que, se encuentra *subjudice* el telégrafo como medio electrónico, aun si bien la Ley Modelo no utilice el término telégrafo.

Si bien el Código de Comercio, dentro de las reformas de mayo de 2000 y agosto de 2003, distingue al telégrafo de los medios electrónicos, ópticos o de cualquier otra tecnología similar para generar mensajes de datos; ello, como se advierte del artículo 80, de dicho ordenamiento legal; también lo es que, supone – como los autores León Tovar Soyla H., González García Hugo, y Vázquez del Mercado Blanco Oscar lo manifiestan-, más a una “falta de técnica”, que a una resistencia por considerar al telegrama como un mensaje de datos; máxime que dada la naturaleza de éste, es considerada información susceptible de ser generada, enviada, recibida, archivada o comunicada por un medio similar a los medios

electrónicos u ópticos.⁷⁶

1.5.4. Correo electrónico.

Es un servicio que se clasifica dentro de los servicios de valor agregado, entendiéndose éstos como aquellos que emplean una red pública de telecomunicaciones y que tienen efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida por algún usuario y, que comercializan a los usuarios información adicional, diferente o reestructurada, o que implican interacción del usuario con información almacenada; ello, atento al artículo 3º, fracción XII, de la Ley Federal de Telecomunicaciones.

El correo electrónico es uno de los servicios más utilizados dentro de Internet. Mediante este servicio se asigna a cada usuario un segmento de la memoria de la computadora del proveedor de servicios (servidor), como depósito para los mensajes (buzón) dirigidos al usuario (destinatario).

El mensaje enviado por una persona a través del correo electrónico, viaja por la red hasta el servidor del proveedor de servicios, en donde el destinatario recupera sus mensajes de manera diferida desde su computadora al conectarse a dicho servidor a través de Internet o por cualquier otro medio de telecomunicación. Una de las características de este servicio es la forma casi instantánea en la cual el correo electrónico llega al destinatario, a diferencia del correo convencional, el cual, aún enviado por mensajería privada tarda varios días.

En México, para que una compañía preste el servicio de correo electrónico a los usuarios sobre una red pública de telecomunicaciones, requiere de una constancia de registro de servicios de valor agregado emitida por la Comisión Federal de Telecomunicaciones.⁷⁷

⁷⁶ Cfr. *Ibidem*, p.p. 58, 64-65.

⁷⁷ Cfr. *Ibidem*, 58-60.

1.5.5. Intercambio electrónico de datos (EDI).

Es un medio electrónico utilizado para generar, enviar, recibir o archivar información. Sus siglas corresponden al inglés *Electronic Data Interchange*. Los tres componentes de un sistema EDI son los mensajes estándar, los programas EDI o las estaciones de usuario, y las (tele)comunicaciones.

El EDI es el envío y recepción de documentos a través de medios telemáticos con el propósito de posibilitar su tratamiento automático. Está considerado este medio como un servicio de valor agregado, en virtud de que proporciona a los usuarios el almacenamiento y envío automatizado de información estructurada bajo un formato definido. Como ejemplo, el intercambio electrónico de datos (EDI) se utiliza en operaciones masivas como órdenes de compra, pedidos, facturación y suscripciones, las cuales permiten a las empresas agilizar, incrementar y facilitar sus operaciones, suprimir grandes costos de papel, ampliar su prestigio, analizar mercados y perspectivas de clientes, etcétera.

La Ley Modelo sobre Comercio Electrónico, define por intercambio electrónico de datos (EDI), la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto.⁷⁸

1.5.6. Fax

Es un medio electrónico por medio del cual se envía información, a través de un dispositivo de comunicación con que cuenta, que transmite imágenes y textos a través de una línea telefónica. Implica el uso de escáner (escandidor), un módem y una impresora; tiene la capacidad de leer una hoja de papel, convirtiendo cada punto en un código numérico. Parecido que un módem, puede convertir estas señales digitales en otro tipo de señal apropiado para viajar por una línea telefónica hasta la

⁷⁸ Cfr. *Ibidem*, págs. 60 y 61.

máquina del fax del destinatario. Al igual que una impresora, recibe las señales para imprimir puntos en la misma posición que estaba la hoja original.⁷⁹

1.5.7. Medios ópticos o similares.

Refiere a cualquier medio por el que se pueda generar, enviar, comunicar, archivar o conservar mensajes de datos, además de los ya conocidos, como el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

Es importante señalar que la Ley Sobre el Comercio Electrónico, establece en su artículo 2, inciso a), la siguiente definición:

“Artículo 2.- - - a) Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, *como pudieran ser, entre otros*, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.”. (resalto)

Esta afirmación que hace la Ley Modelo, al establecer en su parte destacada: *“como pudieran ser, entre otros”*; se interpreta la posibilidad que deja dicha Ley, al surgimiento de otros medios electrónicos además de los existentes.

Lo que robustece, la inoperancia de establecer una lista taxativa, y dejar de lado, los adelantos técnicos y tecnológicos, que pueden generar nuevos medios electrónicos.⁸⁰

1.6. Ley Modelo sobre el Comercio Electrónico de la CNUDMI.

⁷⁹ Cfr. Ibidem, págs. 61 y 62.

⁸⁰ Cfr. Ibidem, p.p. 63-65.

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, aprobó el 12 de junio de 1996, la Ley Modelo sobre el Comercio Electrónico; ello, en virtud del mandato que tiene dicha Comisión, de fomentar la armonización y la unificación progresivas del derecho mercantil internacional, teniendo presente, el interés de todos los pueblos, en particular el de los países en desarrollo en el progreso amplio del comercio internacional; asimismo, nace con el propósito de ayudar de manera significativa a todos los Estados a fortalecer la legislación que rige el uso de métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel y a preparar tal legislación en los casos en que no cuenten con ésta; ello, en observancia al número creciente de transacciones comerciales internacionales que actualmente se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación, habitualmente conocidos como “comercio electrónico”, en los cuales se usan métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel.

La Ley Modelo tiene por objeto enunciar los procedimientos y principios básicos para facilitar el empleo de las técnicas modernas de comunicación para consignar y comunicar información en diversos tipos de circunstancias.

Trata de una ley “marco” que no enuncia por sí sola todas las reglas necesarias para aplicar esas técnicas de comunicación en la práctica; pero, sí facilita el uso del comercio electrónico para el establecimiento de relaciones económicas internacionales armoniosas, y ayuda de manera significativa a todos los Estados a fortalecer la legislación que rige el uso de métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel y a preparar tal legislación, en caso de que no cuenten con ella.

La Ley Modelo no tiene por objeto regular todos los pormenores del empleo del comercio electrónico; por ende, el Estado promulgante puede dictar un reglamento para pormenorizar los procedimientos de cada uno de los métodos autorizados por ésta; ello, a la luz de las circunstancias peculiares y posiblemente variables de cada Estado; por tal, se recomienda que todo Estado que decida

reglamentar más en detalle el empleo de estas técnicas debe procurar no perder de vista la necesidad de mantener la encomiable flexibilidad del régimen de esta Ley.

En ese sentido, la Comisión preparó la “Guía para la incorporación al derecho interno de la Ley Modelo de la CNUMI sobre Comercio Electrónico”, la cual en gran parte está inspirada en los trabajos preparatorios de la Ley Modelo, y donde se destacan los objetivos de esta Ley, así como la explicación de las disposiciones que la contienen.

Esta Guía tiene como propósito facilitar a los órganos ejecutivos y legislativos de los Estados que modernicen su legislación; informa y explica el cómo aplicar la Ley Modelo; mayormente a los Estados poco familiarizados con las técnicas de comunicación reguladas en dicha Ley. Asimismo, la Guía orienta a los Estados en la incorporación de su régimen al derecho interno.

Entre los objetivos de la Ley Modelo, se encuentran los siguientes: a). ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitan eliminar obstáculos jurídicos; b). crear un marco jurídico que permita un desarrollo más seguro de las vías electrónicas de negociación designadas por el nombre de “comercio electrónico”; c). facilitar el empleo de las técnicas de comunicación modernas, dotando al empleo de dichas técnicas de la certeza requerida por el comercio cuando la normativa por lo demás aplicable cree obstáculos a dicho empleo o sea fuente de incertidumbres que no puedan eliminarse mediante estipulaciones contractuales; d). facilitar el empleo de los modernos medios de comunicación y de archivo de la información, basado en el establecimiento de un equivalente funcional para la documentación sobre soporte electrónico; e). ayudar a remediar los inconvenientes que dimanen del hecho de que un régimen legal interno inadecuado, puede obstaculizar el comercio internacional, al depender una parte importante de ese comercio de la utilización de las modernas técnicas de comunicación; f). valioso instrumento en el ámbito internacional, para interpretar ciertos convenios y otros instrumentos internacionales existentes que impongan de hecho algunos obstáculos al empleo del comercio electrónico; g). medio para reconocer la validez del comercio electrónico sin necesidad de tener que negociar un

protocolo para cada uno de esos instrumentos internacionales en particular; y, h). facilitar el empleo del comercio electrónico, a efecto de conceder igualdad de trato a los usuarios de mensajes consignados sobre un soporte informático que a los usuarios de la documentación consignada sobre papel.

Dentro del ámbito de aplicación, la Comisión ha expresado que la Ley Modelo debe considerarse como un régimen especial bien definido y equilibrado que se recomienda incorporar al derecho interno en forma de norma unitaria de rango legal, esto es, se puede incorporar el régimen de la Ley Modelo en una o en varias normas de rango legal, según cuál sea la situación interna de cada Estado. La reconsideración que hizo el Grupo de Trabajo de la Comisión, de formular un texto jurídico redactado en forma de “disposiciones legales modelo”, fue en virtud de que se opinó en general, que el empleo del término “disposiciones legales modelo” podía suscitar incertidumbre sobre la índole jurídica del instrumento; y, si bien hubo cierto apoyo en favor de que se retuviera el término “disposiciones legales modelo”, prevaleció el parecer de que era preferible el término “ley modelo”.

Además, se opinó en general que cabía ahora considerar que las disposiciones legales modelo formaban un régimen equilibrado y bien definido que cabría promulgar conjuntamente como un solo instrumento; no obstante, según la situación imperante en cada Estado que le diera efecto, la Ley Modelo podía incorporarse en forma de ley especial o integrarse en diversas partes de la legislación existente.

Bajo ese esquema, la Comisión ha concluido que los objetivos de la Ley Modelo serán mejor logrados cuanto mayor sea su aplicación; asimismo, afirma que en el futuro tal vez sea preciso regular otras ramas particulares del comercio electrónico, por lo que se ha de considerar a la Ley Modelo citada como un instrumento abierto destinado a ser complementado por futuras adiciones; por lo que, anuncia que tiene previsto mantenerse al corriente de los avances técnicos, jurídicos y comerciales que se produzcan en el ámbito de aplicación de la Ley Modelo y, de juzgarlo aconsejable, introducir nuevas disposiciones modelo en el texto de la misma o modificar alguna de las disposiciones actuales.

Orgánicamente, la Ley Modelo cuenta con 17 artículos, conformada por dos partes; una parte relativa al *Comercio Electrónico general*, y la segunda parte relativa al *Comercio Electrónico en materias específicas*.

Se han promulgado leyes influenciadas por la Ley Modelo de la CNUDMI sobre comercio electrónico, y adoptadas en las fechas que se indican, en: Australia (1999), Brunel Darussalam (2000), Cabo-Verde (2003), China (2004), Colombia (1999), Ecuador (2002), los Emiratos Árabes Unidos (2006), Eslovenia (2000), Filipinas (2000), Francia (2000), Guatemala (2008), India (2000), Irlanda (2000), Jamaica (2006), Jordania (2001), Mauricio (2000), Nueva Zelandia (2002), Pakistán (2002), Panamá (2001), República de Corea (1999), República Dominicana (2002), Singapur (1998), Sri Lanka (2006), Sudáfrica (2002), Tailandia (2002), Venezuela (2001) y Vietnam (2005).

La Ley Modelo también ha sido adoptada en el Bailiwick de Guernesey (2000), el Bailiwick de Jersey (2000) y la Isla de Man (2000), que son dependencias de la Corona del Reino Unido de Gran Bretaña e Irlanda del Norte; en las Bermudas (1999), las islas Caimán (2000), y las Islas Turcos y Caicos (2000), territorios de ultramar del Reino Unido, y en Hong Kong (Región Administrativa Especial de China) (2000).

También, ha tenido influencia la Ley Modelo, en Estados Unidos de América, con la Ley Uniforme de transacciones electrónicas, adoptada en 1999 por la Conferencia Nacional de Comisionados sobre la Ley Uniforme Estatal, promulgada por diversos estados de esta nación; así como en Canadá, con la Ley Uniforme de comercio electrónico, adoptada en 1999 por la Conferencia de Derecho Uniforme del Canadá, promulgada en diversas provincias y territorios. De la misma forma, en México, dicha Ley ha tenido influencia, lo que ha derivado desde el año 2000, adiciones y reformas a diversos ordenamientos legales.⁸¹

Seguido, se reproduce la Ley Modelo de la CNUDMI sobre Comercio Electrónico.⁸²

⁸¹ www.uncitral.org

⁸² www.uncitral.org

“Ley Modelo de la CNUDMI sobre Comercio Electrónico

Primera parte. Comercio electrónico en general

CAPÍTULO I. DISPOSICIONES GENERALES

*Artículo 1. — Ámbito de aplicación**

La presente Ley** será aplicable a todo tipo de información en forma de mensaje de datos utilizada en el contexto*** de actividades comerciales****.

Artículo 2. — Definiciones

Para los fines de la presente Ley:

- a)* Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;
- b)* Por “intercambio electrónico de datos (EDI)” se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;
- c)* Por “iniciador” de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él;
- d)* Por “destinatario” de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a él;
- e)* Por “intermediario”, en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él;
- f)* Por “sistema de información” se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

*La Comisión sugiere el siguiente texto para los Estados que deseen limitar el ámbito de aplicación de la presente Ley a los mensajes de datos internacionales: La presente Ley será aplicable a todo mensaje de datos que sea conforme a la definición del párrafo 1) del artículo 2 y que se refiera al comercio internacional.

**La presente ley no deroga ninguna norma jurídica destinada a la protección del consumidor.

***La Comisión sugiere el siguiente texto para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley: La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en las situaciones siguientes: [...].

****El término “comercial” deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de facturaje (*factoring*); de arrendamiento de bienes de equipo con opción de compra (*leasing*); de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

Artículo 3. — Interpretación

1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

2) Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4. — Modificación mediante acuerdo

1) Salvo que se disponga otra cosa, en las relaciones entre las partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del capítulo III podrán ser modificadas mediante acuerdo.

2) Lo dispuesto en el párrafo 1) no afectará a ningún derecho de que gocen las partes para modificar de común acuerdo alguna norma jurídica a la que se haga referencia en el capítulo II.

CAPÍTULO II. APLICACIÓN DE LOS REQUISITOS JURÍDICOS A LOS MENSAJES DE DATOS

Artículo 5. — Reconocimiento jurídico de los mensajes de datos

No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.

Artículo 5 bis. — Incorporación por remisión

(En la forma aprobada por la comisión en su 31.º período de sesiones, en junio de 1998)

No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.

Artículo 6. — Escrito

- 1) Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta.
- 2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.
- 3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 7. — Firma

- 1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:
 - a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y
 - b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.
- 2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.
- 3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 8. — Original

- 1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:
 - a) Si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

3) Para los fines del inciso a) del párrafo 1):

a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y

b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso. 4) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 9. — Admisibilidad y fuerza probatoria de los mensajes de datos

1) En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos:

a) Por la sola razón de que se trate de un mensaje de datos; o

b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.

2) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 10. — Conservación de los mensajes de datos

1) Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:

a) Que la información que contengan sea accesible para su ulterior consulta; y

b) Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y

c) Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.

2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.

3) Toda persona podrá recurrir a los servicios de un tercero para observar el requisito mencionado en el párrafo 1), siempre que se cumplan las condiciones enunciadas en los incisos a), b) y c) del párrafo 1).

CAPÍTULO III. COMUNICACIÓN DE LOS MENSAJES DE DATOS

Artículo 11. — Formación y validez de los contratos

1) En la formación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos.

2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 12. — Reconocimiento por las partes de los mensajes de datos

1) En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 13. — Atribución de los mensajes de datos

1) Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador. 2) En las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:

a) Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o

b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

3) En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un mensaje de datos proviene del iniciador, y a actuar en consecuencia, cuando:

a) Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o

b) El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

4) El párrafo 3) no se aplicará:

a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o

b) En los casos previstos en el inciso b) del párrafo 3), desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador.

5) Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá actuar en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a algún error en el mensaje de datos recibido.

6) El destinatario tendrá derecho a considerar que cada mensaje de datos recibido es un mensaje de datos separado y a actuar en consecuencia, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos era un duplicado.

Artículo 14. — Acuse de recibo

1) Los párrafos 2) a 4) del presente artículo serán aplicables cuando, al enviar o antes de enviar un mensaje de datos, el iniciador solicite o acuerde con el destinatario que se acuse recibo del mensaje de datos.

2) Cuando el iniciador no haya acordado con el destinatario que el acuse de recibo se dé en alguna forma determinada o utilizando un método determinado, se podrá acusar recibo mediante:

- a) Toda comunicación del destinatario, automatizada o no, o
- b) Todo acto del destinatario, que basten para indicar al iniciador que se ha recibido el mensaje de datos.
- 3) Cuando el iniciador haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo.
- 4) Cuando el iniciador no haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, si no ha recibido acuse en el plazo fijado o convenido o no se ha fijado o convenido ningún plazo, en un plazo razonable el iniciador:
- a) Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y
- b) De no recibirse acuse dentro del plazo fijado conforme al inciso a), podrá, dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener.
- 5) Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente. Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido.
- 6) Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.
- 7) Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo no obedece al propósito de regir las consecuencias jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo.

Artículo 15. — Tiempo y lugar del envío y la recepción de un mensaje de datos

- 1) De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando entre en un sistema de información que no esté bajo el control del iniciador o de la persona que envió el mensaje de datos en nombre del iniciador.
- 2) De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:
- a) Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar:

- i) En el momento en que entre el mensaje de datos en el sistema de información designado; o
 - ii) De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;
- b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar al entrar el mensaje de datos en un sistema de información del destinatario.
- 3) El párrafo 2) será aplicable aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje conforme al párrafo 4).
- 4) De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente párrafo:
- a) Si el iniciador o el destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal;
 - b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.
- 5) Lo dispuesto en el presente artículo no será aplicable a: [...].

Segunda parte. Comercio electrónico en materias específicas

CAPÍTULO I. TRANSPORTE DE MERCANCÍAS

Artículo 16. — Actos relacionados con los contratos de transporte de mercancías

Sin perjuicio de lo dispuesto en la parte I de la presente Ley, el presente capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea exhaustiva:

- a) i) indicación de las marcas, el número, la cantidad o el peso de las mercancías;
 - ii) declaración de la índole o el valor de las mercancías;
 - iii) emisión de un recibo por las mercancías;
 - iv) confirmación de haberse completado la carga de las mercancías;
- b) i) notificación a alguna persona de las cláusulas y condiciones del contrato;
 - ii) comunicación de instrucciones al portador;

- c)
 - i) reclamación de la entrega de las mercancías;
 - ii) autorización para proceder a la entrega de las mercancías;
 - iii) notificación de la pérdida de las mercancías o de los daños que hayan sufrido;
- d) cualquier otra notificación o declaración relativas al cumplimiento del contrato;
- e) promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;
- f) concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;
- g) adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

Artículo 17. — Documentos de transporte

- 1) Con sujeción a lo dispuesto en el párrafo 3), en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 16 se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.
- 2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento.
- 3) Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío, o la utilización, de un documento, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.
- 4) Para los fines del párrafo 3), el nivel de fiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.
- 5) Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 16, no será válido ningún documento utilizado para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos. Todo documento que se emita en esas circunstancias deberá contener una declaración a tal efecto. La sustitución de mensajes de datos por documentos no afectará a los derechos ni a las obligaciones de las partes.

6) Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia, en un documento, esa norma no dejará de aplicarse a un contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en un documento.

7) Lo dispuesto en el presente artículo no será aplicable a: [...].”

1.7. Equivalencia funcional

En sentido estricto, equivalencia funcional, es dar el mismo tratamiento que se da al documento electrónico que al documento escrito, a fin de evitar, como lo menciona el autor Nelson Remolina Angarita, que la validez de una comunicación electrónica o de cualquier documento electrónico se supedite a su reproducción a un medio físico.⁸³

El equivalente funcional, “se basa en un análisis de los objetivos y funciones del requisito tradicional con miras a determinar la manera de satisfacer sus objetivos y funciones en el contexto tecnológico.”⁸⁴

Se busca dar el mismo reconocimiento al documento electrónico, que se le da a un documento de papel; ello, a través de procedimientos que aseguren niveles similares de seguridad, confiabilidad y transparencia.

El proceso por el que un documento de papel es transformado en un documento electrónico, se le llama desmaterialización.⁸⁵

Ello, da lugar a la desaparición de aquella conexión permanente entre el papel y derecho (incorporación), propia de los títulos de crédito constitutivos.⁸⁶

⁸³ Cfr. Universidad de los Andes, Facultad de Derecho, Internet, ob. cit. pág. 13.

⁸⁴ Ídem.

⁸⁵ Cfr. Universidad de los Andes, Facultad de Derecho, Internet, ob. cit. pág. 23.

⁸⁶ Cfr. León Tovar, Soyla H., y González García Hugo, *Derecho Mercantil*, Oxford University Press México, Sociedad Anónima de Capital

La desmaterialización puede ser *total* o *parcial*. Es total, cuando el documento es creado, circulado y negociado electrónicamente, sin que el mismo sea producto de la transformación de un documento de papel a un documento electrónico. Es parcial, cuando el documento es creado en forma física pero las transacciones sobre éste se realizan electrónicamente. En este caso, usualmente el documento de papel es depositado en un Banco o en una central de registro donde es convertido en documento electrónico para realizar operaciones sobre el mismo.⁸⁷

Se ha criticado la utilización del termino desmaterialización, en virtud de que se señala que sólo puede desmaterializarse lo que previamente esta dotado de materia; por lo que, para los casos en que el documento ha sido creado previamente en papel y luego transformado a documento electrónico, se dice que el documento fue *desmaterializado*; y, cuando el documento fue creado electrónicamente, nos encontramos con un documento *inmaterializado*.⁸⁸

La Ley Modelo de la CNUDMI sobre Comercio Electrónico, sigue un nuevo criterio, denominado a veces “criterio del equivalente funcional”, basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico.

En dicho análisis, la CNUDMI establece que el documento en papel cumple funciones como: proporcionar un documento legible para todos; asegurar la inalterabilidad de un documento a lo largo del tiempo; permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito; permitir la autenticación de los datos consignados suscribiéndolos con una firma; y, proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales.

Variable, México, 2007, p.p. 171.

⁸⁷ Cfr. Universidad de los Andes, Facultad de Derecho, Internet, ob. cit, pág. 25.

⁸⁸ Cfr. Ídem.

Derivado de lo anterior, afirma la citada Comisión que, la documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, mucha mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos; por lo que, agrega, que la adopción de este criterio del equivalente funcional, no debe dar lugar a que se impongan normas de seguridad más estrictas a los usuarios del comercio electrónico (con el consiguiente costo) que las aplicables a la documentación consignada sobre papel.

Sigue aportando la Comisión que, un mensaje de datos, que es una forma de documento electrónico, no es de por sí, el equivalente de un documento de papel, ya que es de naturaleza distinta; sin embargo, se adopta en la Ley Modelo un *criterio flexible* que tiene en cuenta la graduación actual de los requisitos aplicables a la documentación consignada sobre papel.

Esto es, al adoptar el criterio del “equivalente funcional”, la CNUDMI prestó atención a los requisitos de forma (escrito, firma y original), para los mensajes de datos, para efecto de dotarlos del mismo grado de fiabilidad, inalterabilidad y rastreabilidad que a los documentos de papel.

Esto se encuentra plasmado en los artículos 6° a 8° de la Ley Modelo, de cuyo contenido se advierte lo siguiente:

- Cuando la ley requiera que la información conste por *escrito*, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta, ya sea que el requisito en él previsto está expresado en forma de obligación, o que la ley simplemente prevea consecuencias en el caso de que la información no conste por escrito.
- Cuando la ley requiera la *firma* de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: *i*). Si se utiliza un

método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y, *ii*). Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

- Cuando la ley requiera que la información sea presentada y conservada en su forma *original*, ese requisito quedará satisfecho con un mensaje de datos: *i*). exista alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma. La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y el grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso; y, *ii*). si se requiere que la información sea presentada, que pueda ser mostrada a la persona a la que se deba presentar.

En esa tesitura, el legislador mexicano, al reformar el Código de Comercio en agosto de 2003, tuvo en cuenta estos requisitos de la Ley Modelo, y los plasmó en los artículos 93 y 93 Bis (Adición publicada en el Diario Oficial de la Federación el 29 de agosto de 2003); éste vinculante con el artículo 49, del código mercantil citado, los cuales a la letra dicen:

“Artículo 93. Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.- - - Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a

dichas partes.- - En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de Mensajes de Datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.”

“**Artículo 93 Bis.** Sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos: I. Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma, y II. De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.- - - Para efectos de este artículo, se considerará que el contenido de un Mensaje de Datos es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.”

“**Artículo 49.** Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignent contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la

Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.”

Así, quedan satisfechos los requisitos jurídicos a los mensajes de datos, para que opere la equivalencia funcional en la legislación. Lo que representa un gran avance en materia de equivalencia funcional en nuestro país.

2. Aplicaciones del comercio electrónico.

2.1. Utilidad en la práctica y ventajas

Es indudable que el comercio electrónico, incide en el fenómeno globalizador actual en el mundo. Creo que en la medida en cómo se utilice esta herramienta, es como se pueden generar ventajas o desventajas; **“retener lo bueno y desechar lo malo”**.

Como acertadamente lo refieren las autoras Cavazos Arroyo Judith y Reyes Guerrero Soraya, esta nueva práctica comercial de trascendencia económica actual incide en el suceso económico llamado globalización, que ha conllevado a un impacto en la economía, política, cultura y social en el mundo; impulsado éste por la revolución tecnológica, la apertura comercial y el neoliberalismo; por lo que, concluyen que nuestra tarea es analizarla y decidir la forma en que participaremos en ella a fin de obtener el mayor provecho en bien.⁸⁹

A continuación, se exponen algunas opiniones que hacen diversos autores sobre el impacto que ha tenido el fenómeno globalizador, el cual, indudablemente acoge al comercio electrónico; de las cuales comparto alguna y, en otras, adoptaré alguna consideración oportuna.

Desde el punto de vista **económico**, algunos autores señalan que el fenómeno globalizador ha tenido impacto en:

⁸⁹ Cfr. Cavazos Arroyo, Judith y Reyes Guerrero, Soraya, ob. cit, pág. 105.

- Bajos costos de transporte y seguimiento de embarques.
- Formas de producción más ágiles.
- Flujos activos y libres de capital.
 - El Estado se ha transformado en un “catalizador” de actividades económicas, en vez de ser un regulador de las mismas.
 - Intangibilidad de los productos.
 - Descentralización de centros fabriles.
 - Incremento en el consumo de artículos de origen extranjero.
 - Crecimiento del comercio internacional.
 - Inequitativa distribución de la riqueza.
 - Toma de decisiones “en tiempo real” vía electrónica.
 - Integración de mercados financieros.
 - Competencia agresiva en extremo.⁹⁰

En el aspecto **político**, se establece que el fenómeno globalizador ha tenido como efecto, los siguientes:

- “Pérdida” de autoridad económica del gobierno de cada país. Las leyes del mercado digital cobran “supremacía”.
- Conformación de bloques político-económicos de donde surgen las grandes decisiones o tendencia.
- Crecimiento de entidades paralelas a las gubernamentales que ejercen presión.⁹¹

No estoy de acuerdo con el primer punto de este apartado, pues considero que el Estado sí tiene autoridad, y por ende, es regulador y rector de todas y cada una de las actividades económicas; tan es así, la injerencia internacional de la mayoría de los Estados en materia de comercio electrónico, que ha dado origen a la uniformidad legislativa en la mayoría de las naciones. Si bien es cierto actualmente falta por regular distintos aspectos del comercio electrónico o mercado digital, también lo es

⁹⁰ Cfr. *Ibidem*, p.p. 106.

⁹¹ Cfr. *Ibidem*, p.p. 107.

que nada está por encima de la ley, y por ende, nada por encima de la rectoría del Estado; por lo que, tarde o temprano las actividades comerciales que aún no se encuentran reguladas, un día se sujetarán a la autoridad del Estado.

Al respecto, en el país se encuentra como fundamento, el artículo 25 de la Constitución Política de los Estados Unidos Mexicanos, el cual, en su parte conducente establece lo siguiente:

“**Artículo 25.** Corresponde al Estado la rectoría del desarrollo nacional para garantizar que éste sea integral y sustentable, que fortalezca la Soberanía de la Nación y su régimen democrático y que, mediante el fomento del crecimiento económico y el empleo y una más justa distribución del ingreso y la riqueza, permita el pleno ejercicio de la libertad y la dignidad de los individuos, grupos y clases sociales, cuya seguridad protege esta Constitución.”.

En el área **laboral**, diversos autores establecen que la globalización ha conllevado a las siguientes consecuencias, a saber:

- Nuevos retos para el sindicalismo.
- Perfil especializado de trabajadores.
- Trabajos desde casa con horarios flexibles.
- Contrataciones transnacionales.⁹²

Asimismo, en el área **sociocultural**, este fenómeno económico ha desarrollado los siguientes:

- Ha promovido la innovación.
- Agrupaciones virtuales.
- Educación global.
- Fomento del individualismo.
 - Pérdida de identidad nacional. Copia de manifestaciones culturales ajenas.

⁹² Cfr. *Ibidem*, págs. 107 y 108..

- Diferentes procesos de socialización.
 - Marginación y exclusión de quienes no tiene acceso a la economía digital.⁹³

Sobre este último punto, considero que el Estado debe crear los instrumentos, en donde a través de programas sociales, se distribuyan de manera gratuita, las tecnologías de información y, por ende, se enseñe sobre la utilización de éstas; a efecto de que dichas poblaciones tengan acceso a la información; la cual, ha pasado a ser un derecho humano, a ser una *garantía individual*. Asimismo, se utilicen estas tecnologías, para efecto de promover y reactivar la venta de los productos elaborados en esas zonas al extranjero por medio de Internet.

Respecto de los factores que impulsan el desarrollo del comercio electrónico, se enuncian los siguientes:

- Apertura de mercados nacionales: Libre comercio.
- Fusiones entre empresas: Multinacionales.
- Eliminación de empresas públicas: Privatizaciones.
- Desregulación financiera internacional a favor del libre comercio: TLC.

Como beneficios, se han apuntado los siguientes temas:

- Eficacia del mercado que disminuye los monopolios.
- Mejoras en la comunicación y cooperación internacional, que lleva a mejor aprovechamiento de los recursos.
- Impulso desarrollo científico-técnico.
- Mayor capacidad de maniobra frente a fluctuaciones de las economías nacionales.
- Eliminación de las barreras de entrada del mercado laboral, financiero y de bienes y servicios.
- Reducción de precios.

⁹³ Cfr. *Ibidem*, p.p. 108.

- Más empleos.
- Incremento en la producción.
- Los derechos de las mujeres ha avanzado.
- La tasa de alfabetización mundial aumentó del 52% al 81%.

Como riesgos y críticas, algunos actores enuncian los siguientes:

- Privatización de los sectores económicos.
- Aumento de la competencia.
- Acceso irregulado de los países a los mercados internacionales.
- Pérdida de la identidad nacional por el intercambio cultural.
- Materialismo.
- Desplazamiento de empresas locales por empresas multinacional.
- Aumento de desequilibrios económicos, sociales y territoriales.
- Descuido sobre los índices de desarrollo humano.

En atención a los riesgos y críticas citadas, considero conveniente destacar al materialismo, el cual, si es tratado con un ánimo de buscar riqueza, puede irrumpir con el desarrollo de las relaciones humanas, así como con la pérdida del sentido de ver por la necesidad de los demás.

Concluyo al respecto, que no se debe perder de vista un sentido de cooperación internacional, y ayuda mutua. Dirigir los esfuerzos siendo solidarios; cuyo propósito sea el fortalecimiento unánime de las economías de las naciones.

Es un reto, pero creo se puede lograr, a pesar de los obstáculos que se presentan, como el régimen socialista, o las extremas condiciones que presentan algunos países.

Sin embargo, no podemos ver hacia atrás. Tenemos que trabajar hacia una renovación de nuestra mente, con ánimo solidario. Lo que hoy impera mundialmente

es el fenómeno globalizador, del cual creo se puede sacar el mayor provecho y, bajo ese tenor, crear una nueva conciencia de cooperación internacional.

2.2. Medios de pago electrónico (EPS)

Los medios de pago electrónico, refieren a nuevos sistemas o formas de pago, a través de vías telemáticas, los cuales deben ofrecer seguridad y confiabilidad.

Como lo señala la autora Andrea Viviana Sarra: “El comercio electrónico en cualquiera de sus dos modalidades –directo e indirecto–, requiere de métodos de pago digital instantáneo, especialmente cuando se trata de transacciones de pequeños montos y los potenciales consumidores son anónimos, y están distribuidos por todo el mundo.”⁹⁴

“Los medios de pago electrónico son aquellos sistemas que permiten el procesamiento de órdenes de pago a través de sistemas electrónicos.”⁹⁵

Cabe mencionar al autor Martínez Nadal Apol.Ionia, quien hace un estudio sobre los medios de pago en el comercio electrónico, y expresa que en los primeros tiempos del comercio electrónico en Internet, las tarjetas tradicionales de crédito y débito se han convertido en medio habitual de pago, utilizando, a efectos de seguridad, protocolos de comunicaciones existentes (SSL) o desarrollando otros destinados específicamente al comercio electrónico (SET); no obstante, sigue expresando el citado autor, que el pago mediante tarjeta presenta diversos inconvenientes, esto es, no se presenta el anonimato del comprador e implica un coste excesivo para las transacciones de pequeña cuantía; en ese sentido, concluye el citado autor, que en los últimos tiempos han surgido propuestas de creación de dinero electrónico almacenado en Software del ordenador y también las tarjetas monedero que almacenan valores monetarios en un chip y resultan adecuados para las

⁹⁴ Viviana Sarra, Andrea, *Comercio electrónico y derecho*, Editorial Astrea de Alfredo y Ricardo Depalma, Argentina, 2000, p.p. 409.

⁹⁵ García Más, Francisco Javier, *Comercio y Firma Electrónicos (Análisis Jurídico de los Servicios de la Sociedad de la Información)*, editorial Lex Nova, Sociedad Anónima, Segunda edición, España, 2004, p.p. 332.

transacciones de escaso valor.⁹⁶

Al efecto, dicho autor hace una relación de diversos medios electrónicos, a saber:

- a. **Sistemas sin tarjeta**, es dinero electrónico en sentido estricto. Se substituye el soporte tradicional por el soporte electrónico, esto es substituyendo el papel por bits. El medio de pago creación del criptógrafo David Chaum basado en Software que permite a sus usuarios enviar dinero electrónico en pago de las compras realizadas desde cualquier ordenador a otro, utilizando cualquier red de comunicación, incluida Internet, y que pretende preservar el anonimato del comprador.
- b. **Micropagos**, es utilizado como alternativa económica a los medios de pago con tarjeta, basados en la existencia de cupones electrónicos que representan dinero con los que el comprador paga al vendedor.
- c. **Tarjetas monederos** o monedero electrónico, es una tarjeta que incorpora un chip en el que se almacena un valor monetario prepagado que puede ser gastado en cualquier comercio con lector de tales tarjetas. El titular de la tarjeta puede cargarla de dinero en cualquier terminal de carga.⁹⁷

Como lo concluye el autor Miguel Ángel Dávora Rodríguez: “La utilización de las nuevas tecnologías de la información como medio en el cumplimiento de las obligaciones, no puede todavía definirse en una forma detallada porque eso podría llevar, incluso, a una limitación en el desarrollo de esta actividad electrónica.”⁹⁸

⁹⁶ Cfr. Ídem.

⁹⁷ Cfr. Ídem.

⁹⁸ Davara Rodríguez, Miguel Ángel, ob. cit, p.p. 350.

La Unión Europea, se ha expresado sobre los sistemas seguros de pago en relación con el comercio electrónico, como lo indica en la Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre comercio electrónico y servicios financieros de 7 de febrero de 2001; la cual se transcribe textualmente a continuación:

“La seguridad de los pagos es fundamental para el desarrollo del comercio electrónico entre empresas y consumidores. Hoy en día no existe un método generalizado de pago transfronterizo en Internet que sea eficaz, seguro y barato. Los consumidores no confían en la seguridad de los pagos de Internet, y su inquietud se ha visto reforzada por una serie de graves errores en la prestación de servicios financieros en línea (...) Las tarjetas de pago son hoy un día el instrumento más extendido de pago en línea; entre los demás figuran los sistemas de pago electrónico en Internet basados en monederos digitales (“ciberdinero”) o en sistemas contables. El marco legislativo garantiza cierta protección a los consumidores, pero no ofrece respuesta satisfactoria a buen número de problemas que plantea el comercio en línea en la Comunidad. La diversidad de disposiciones nacionales acentúa además el riesgo de la fragmentación legislativa del mercado interior. Son precisas mejoras de la seguridad técnica y la creación de “redes de seguridad” legislativas en caso de problemas de pago...”. “... En materia de seguridad técnica la iniciativa de la Comisión e-Europe fomenta la utilización de las nuevas técnicas, incluido un plan de acción sobre tarjetas inteligentes, y contempla ulteriores trabajos sobre técnicas de identificación y autenticación. Las tarjetas inteligentes, por ser propiedad personal, suelen considerarse privadas y seguras y, en consecuencia, se juzgan un medio fiable de almacenar y transferir datos. Además, las tarjetas inteligentes permiten acceder a servicios y aplicaciones electrónicas. La propuesta de Decisión marco sobre la lucha contra el fraude y falsificación de medios de pago distintos del efectivo contempla la tipificación de tales actividades como delitos en toda la unión. En una Comunicación al respecto, la Comisión propone una serie de medidas (estudio de las características de seguridad de las nuevas soluciones de pago en el comercio electrónico, intercambio de información, formación y suministro de material pedagógico) a fin de disuadir a los infractores, y reforzar la confianza de los consumidores...- - - En Estados Unidos, la legislación marco en este ámbito atribuye a las principales

empresas internacionales de tarjetas de pago un papel fundamental a efectos de protección del consumidor por medio de su sistema de “reembolsabilidad” (chamberback). En la Unión, salvo algunas excepciones, estos mecanismos creados por el sector no suelen basarse en la legislación nacional, sino que se regulan por el contrato celebrado entre el banco emisor de la tarjeta y el banco del comerciante conforme al reglamento de la empresa de tarjetas. La decisión de iniciar el procedimiento de reembolso por denuncia del titular de la tarjeta queda en manos del banco emisor. Así pues, no existe una base legislativa coherente que regule los reembolsos en el mercado interior. Es indudable que ello perjudica al funcionamiento de los procedimientos de reembolso, en particular en las transacciones transfronterizas...”. “... Es pues urgente establecer a escala comunitaria un marco legislativo que establezca el derecho de reembolso en caso de transacción no autorizada o de no entrega y que especifique las condiciones para el mismo (...). A fin de limitar el riesgo de recurso abusivo a los sistemas de reembolso, es fundamental que los comerciantes de un Estado miembro dispongan de sistemas que permitan comprobar la identidad de los consumidores de otro...”⁹⁹

Otro medio de pago electrónico, es a través de la *banca digital*, definida ésta como la provisión de servicios y productos bancarios por medio de canales digitales. Se caracteriza por dos aspectos: i). la naturaleza de los canales de transferencia, los cuales pueden ser: redes cerradas, de acceso restringido a los participantes del sistema, por lo que están limitadas a los términos de los acuerdos previos entre partes, o redes abiertas, que no tienen ningún tipo de restricción, ejemplo: Internet; y, ii). los medios por los cuales los clientes tiene acceso a esos canales, en donde los dispositivos más usados son: a) terminales de venta; b) cajeros automáticos (ATM); teléfono; c) computadoras personales; d) dispositivos portables; y, e) “tarjetas inteligentes.”¹⁰⁰

2.3. El dinero electrónico

⁹⁹ García Más, Francisco Javier, ob. cit, p.p. 333.

¹⁰⁰ Viviana Sarra, Andrea, ob. cit, pág. 410.

Como modalidades del dinero electrónico, se pueden citar las siguientes:

a. Dinero *on line*. Requiere interactuar con el banco (por módem o red) para llevar a cabo una transacción con una tercera parte. Esta modalidad incluye las *tarjetas de crédito* y el *Saf-T-Pay*.

- *Tarjetas de Crédito*. Es utilizada para pagar transacciones electrónicas. Tiene la ventaja de permitir al consumidor pagar en cualquier sitio web sin importar la moneda en que está expresando el importe, en virtud de que la conversión se realiza de manera automática. Cuentan con el estándar de encriptación SET (Secure Electronic Transaction), liderado por Visa y MasterCard o por SSL (Secure Socket Layer) de Netscape Communications Corp, para evitar que al entregar el número de tarjeta en cada compra, se deje huella fácil de seguir y que permita recabar información acerca del consumidor.
- *Saf-T-Pay*. Es un sistema de pago que sin necesidad de un nuevo instrumento o clave, una vez que el cliente elige una compra. *Saf-T-Pay* facilita la cantidad en moneda local y el pago electrónicamente por medio de su banco.

b. Dinero *off line*. Se dispone del dinero en la propia computadora y puede gastarse cuando se desee, sin necesidad de contactar para ello con un banco. Dentro del dinero *off line*, se encuentra:

- *Cajeros Electrónicos*. Sistema de dinero electrónico que permite al cliente depositar dinero en una cuenta en una entidad de Internet, para efecto de poder usar ese dinero para adquirir bienes o servicios por Internet con un código alfanumérico asociado a su identidad (sus datos personales proporcionados a la entidad), que le permita adquirir, de los vendedores asociados a las entidades, bienes o servicios.

- Los “cheques electrónicos” (autorizaciones electrónicas). Se integran con una autorización generada, firmada y certificada para disponer de dinero de la cuenta del autorizante. Contienen la misma información que un cheque tradicional y su funcionamiento es el mismo; el emisor usa su chequera electrónica, emite el documento a favor del beneficiario y lo envía por medios electrónicos. El cheque tiene un sistema debit based.

- *e-Cash*. En funcionamiento desde 1994. Es un concepto de pago que surge de la firma Digicash. Es un software que adquiere el usuario. No tiene apariencia física. La compañía pionera que provee este servicio es eCash Technologies, Inc. Esta modalidad se emplea en micropagos, en donde la transacción permite mantener el anonimato del usuario y tener seguridad de autenticidad en virtud al uso de las firmas electrónicas. Los tres elementos que la integran son: el banco emisor, que valida la transacción y que cambia dinero real en virtual; los compradores, que obtienen su tarjeta prepago en el banco en el cual tiene una cuenta aperturada; y, los vendedores, que aceptan el e-cash. Como desventajas de esta modalidad se encuentra que, no todos los bancos están afiliados al sistema Digicash, ni tampoco todos los comercios virtuales; por tanto, se debe navegar en busca de quien acepte esta clase de dinero; no obstante, los beneficios son más.

- *Netcash*. Es un sistema similar al e-cash, desarrollado por el Sciences Institute of the University of Southern California, y consiste en un mecanismo conectado a varios servidores de moneda (currency servers) que hacen posible cambiar en dinero electrónico algunas otras formas de pago, como los cheques electrónicos.¹⁰¹

De lo anterior, se dilucida que se siguen perfeccionando los medios de pago electrónico, en la medida de los avances tecnológicos, y en el interés que adopte cada

¹⁰¹ León Tovar, Soyla H., González García Hugo, ob. cit, p.p. 185.

Estado, por innovar su legislación sobre estos métodos de pago.

Se renuevan las tecnologías, y surgen nuevos retos. Esto es lo interesante.

2.4. La transferencia electrónica

Se ha definido la transferencia electrónica o llamada *transferencia electrónica de fondos interbancarios*, como el envío electrónico de dinero de una cuenta de cheques o tarjeta de débito de un Banco a una cuenta de cheques o tarjeta de débito en cualesquiera de las instituciones bancarias ubicadas dentro del territorio nacional. Tanto quien envía y recibe la transferencia, deben contar con una cuenta de cheques o una tarjeta de débito, lo que permite al cliente de un banco hacer pagos o enviar fondos desde su cuenta a una cuenta en otro banco, o bien, enviar una transferencia electrónica a una cuenta de cheques o ahorros de otro banco radicada en una sucursal en cualquier lugar del país.¹⁰²

Es importante puntualizar lo que el autor Miguel Ángel Davara Rodríguez señala, al diferenciar la transferencia electrónica, como *forma de pago* y como un *simple depósito de dinero*, al expresar que no toda transferencia de fondos es un pago electrónico.¹⁰³

Así, la transferencia electrónica de fondos incide en una actividad económica por medios electrónicos, el cual, puede tratarse de un simple depósito, o bien, de un pago liberatorio de deuda.¹⁰⁴

En México, la Secretaría de Hacienda y Crédito Público, es quien autoriza la realización en forma habitual y profesional de las operaciones que se lleven a cabo mediante transferencia o transmisión de fondos con el público dentro del territorio nacional, tal y como lo redacta los numerales 1º y 181, de la Ley General de Organizaciones y Actividades Auxiliares del Crédito, la cual regula la organización y

¹⁰² www.abm.org.mx

¹⁰³ Cfr. Davara Rodríguez, Miguel Ángel, *Manual de Derecho Informático*, ob. cit. p.p. 301.

¹⁰⁴ Cfr. *Ibidem*, p.p. 302.

funcionamiento de las organizaciones auxiliares del crédito y se aplica al ejercicio de las actividades que se reputan en la misma como auxiliares del crédito; donde la Secretaría de Hacienda y Crédito Público es el órgano competente para interpretar a efectos administrativos los preceptos de esta ley y, en general, para todo cuanto se refiera a las organizaciones y actividades auxiliares del crédito. Dichos dispositivos a la letra dicen, respectivamente:

“**Artículo 1o.** La presente Ley regulará la organización y funcionamiento de las organizaciones auxiliares del crédito y se aplicará al ejercicio de las actividades que se reputen en la misma como auxiliares del crédito. La Secretaría de Hacienda y Crédito Público será el órgano competente para interpretar a efectos administrativos los preceptos de esta Ley y, en general, para todo cuanto se refiera a las organizaciones y actividades auxiliares del crédito.”.

“**Artículo 81.** Se requerirá autorización de la Secretaría de Hacienda y Crédito Público, para realizar en forma habitual y profesional operaciones de compra, venta y cambio de divisas, incluyendo las que se lleven a cabo mediante transferencia o transmisión de fondos, con el público dentro del territorio nacional, excepción hecha de los casos previstos en este artículo y en el artículo 81-A.”.

“**Artículo 81-A.** No se requerirá la autorización a que se refiere el artículo anterior cuando única y exclusivamente se realicen con divisas las operaciones siguientes: I. Compra y venta de billetes así como piezas acuñadas y metales comunes, con curso legal en el país de emisión, hasta por un monto equivalente no superior a diez mil dólares diarios de los Estados Unidos de América por cada cliente;- - - II. Compra y venta de cheques de viajero denominados en moneda extranjera, hasta por un monto equivalente no superior a diez mil dólares diarios de los Estados Unidos de América por cada cliente;- - - III. Compra y venta de piezas metálicas acuñadas en forma de moneda, hasta por un monto equivalente no superior a diez mil dólares diarios de los Estados Unidos de América por cada cliente, y- - - IV. Compra de documentos a la vista denominados y pagaderos en moneda extranjera, a cargo de entidades financieras hasta por un monto equivalente no

superior a diez mil dólares diarios de los Estados Unidos de América por cada cliente. Estos documentos sólo podrán venderlos a las instituciones de crédito y casas de cambio;- - - V. (DEROGADA, D.O.F. 1 DE JUNIO DE 2001).- - - En la celebración de las operaciones descritas en las fracciones I a IV anteriores, el contravalor deberá entregarse en el mismo acto en que se lleven a cabo y únicamente podrán liquidarse mediante la entrega de efectivo, cheques de viajero o cheques denominados en moneda nacional, sin que en ningún caso se comprenda la transferencia o transmisión de fondos.”.

Asimismo, el Banco de México, es el encargado de regular el servicio de transferencia de fondos, a través de instituciones de crédito y de otras empresas que lo presten de manera profesional; ello, atento al artículo 31, de la Ley del Banco de México; cuyo tenor es el siguiente:

“Artículo 31. El Banco Central podrá regular el servicio de transferencias de fondos a través de instituciones de crédito y de otras empresas que lo presten de manera profesional.”.

Actualmente, el Banco de México, ha desarrollado el SPEI (Sistema de Pagos Electrónicos Interbancarios). Este sigue los lineamientos que a continuación se expresan:

- 1) El Ordenante es la persona que desea transferir dinero desde su cuenta bancaria.
- 2) El Beneficiario es la persona que recibe el dinero de la transferencia directamente en su cuenta bancaria.
- 3) El Banco Emisor es el banco comercial que le lleva la cuenta al Ordenante.
- 4) El Banco Receptor es el banco comercial que le lleva la cuenta al Beneficiario.

- 5) El Banco de México es el banco central de la nación, y actúa como “puente” entre el Banco Emisor y el Banco Receptor ya que ambos mantienen una cuenta en el banco central.¹⁰⁵

La transferencia a través del SPEI funciona de la siguiente forma:

- 1) El Ordenante instruye a su Banco Emisor que transfiera dinero, a través de su banca por Internet. La instrucción debe indicar el monto de la transferencia y los datos del Beneficiario, como lo son su cuenta CLABE (18 dígitos) o su número de tarjeta de débito (16 dígitos), su nombre y el de su Banco Receptor. El Ordenante también tiene la opción de incluir alguna referencia (7 dígitos) o concepto (40 letras o dígitos) para una mejor identificación de la transferencia.
- 2) Al recibir la instrucción, el Banco Emisor verifica la identidad de su cliente Ordenante y que el saldo en su cuenta sea suficiente para cubrir la transferencia; aceptando sólo procesar las transferencias que cumplan estos requisitos. En tal caso, el Banco Emisor le avisa al Ordenante, a través de Internet, la hora precisa en que aceptó la transferencia, así como una clave de identificación única, llamada “número de rastreo”, que servirá para futuras aclaraciones.
- 3) Unos minutos después, el Banco Emisor transmite, a través del SPEI, toda la información de la transferencia al Banco de México.
- 4) Al recibir la información, el Banco de México transfiere el dinero de la cuenta que le lleva al Banco Emisor hacia la cuenta que le lleva al Banco Receptor y retransmite toda la información necesaria al Banco Receptor.
- 5) De esta manera el Banco Receptor cuenta con la información necesaria y los recursos para depositarios a favor del Beneficiario.¹⁰⁶

¹⁰⁵ www.blog.banregio.com

¹⁰⁶ Ídem.

Por otro lado, en materia de transferencia electrónica internacional de fondos u orden de pago internacional, México ha celebrado diversos acuerdos en materia de inversiones, y contra la corrupción, los cuales han dado avances sobre el tema de transferencias de fondos internacionales, entre otros, cabe destacar los siguientes: **“Acuerdo Entre el Gobierno de los Estados Unidos Mexicanos y el Gobierno de la Republica Italiana para la Promoción y Protección Reciproca de las Inversiones”**, y la **“Convención de las Naciones Unidas contra la Corrupción, adoptada en la Ciudad de Nueva York, el treinta y uno de octubre de dos mil tres”**.

El “Acuerdo Entre el Gobierno de los Estados Unidos Mexicanos y el Gobierno de la Republica Italiana para la Promoción y Protección Reciproca de las Inversiones”, publicado en la Primera Sección del Diario Oficial de la Federación, el 17 de enero de 2003., y aprobado por la Cámara de Senadores del Honorable Congreso de la Unión, el 17 de abril de 2000, según decreto publicado en el Diario Oficial de la Federación del 10 de julio del propio año; tiene como propósito, la promoción y la mutua protección de las inversiones entre las partes contratantes.

Por otra parte, la “Convención de las Naciones Unidas contra la Corrupción, adoptada en la Ciudad de Nueva York, el 31 de octubre de 2003”, publicada en la Primera Sección del Diario Oficial de la Federación, el miércoles 14 de diciembre de 2005, y aprobada por la Cámara de Senadores del Honorable Congreso de la Unión, el 29 de abril de 2004, según decreto publicado en el Diario Oficial de la Federación del 27 de mayo del propio año; tiene como propósito, prevenir, detectar y disuadir con mayor eficacia las transferencias internacionales de activos adquiridos ilícitamente y a fortalecer la cooperación internacional para la recuperación de activos,

Asimismo, se encuentra la *nómina interbancaria*, que se ha definido como el servicio de transferencias electrónicas de fondos que facilita a los patrones realizar los pagos a sus empleados o pensionados, en cualesquiera de las instituciones bancarias que estos hayan elegido, dentro del territorio nacional; ello, sin importar en

que banco tenga el patrón o el empleado su cuenta.

Los beneficios de la nómina interbancaria, son que facilita la conciliación automática; elimina el riesgo de manejar cheques; elimina el servicio de entrega de cheques a los empleados; minimiza el riesgo de custodia de documentos; minimiza trámites administrativos; reduce costos operativos; reduce la necesidad de manejar efectivo, etcétera.

Las operaciones que se pueden efectuar, a través de ésta, son:

- Pagar la cuenta de una tarjeta de crédito.
- Pagar una obligación a un acreedor en su tarjeta bancaria.
- Pagar a los proveedores de su empresas en cuentas en distintos bancos.
- Pagar los sueldos de sus empleados en las cuentas bancarias que ellos designen.
- Depositar dinero en cuentas bancarias de sus familiares en los distintos bancos.

Esta modalidad de pago ha sido empleada en esquemas de B2B; en la cual, interviene la existencia del software, hardware y vínculos especializados entre las partes vinculantes.

2.5. Comercio electrónico marítimo

Dada la extensión del comercio electrónico, de igual forma en materia de navegación y comercio marítimos tiene injerencia esta nueva modalidad de comercio.

La CNUDMI señala en la Guía para la incorporación al derecho interno de la Ley Modelo sobre Comercio Electrónico, que al preparar dicha Ley, la Comisión tomó nota de que el transporte de mercancías era la rama comercial en la que era más

probable que se recurriera a las comunicaciones electrónicas; por lo que, era necesario un marco jurídico que facilitara el empleo de esos medios de comunicación.

En esa tesitura, fueron plasmados los actos relacionados con los contratos de transporte de mercancías, en los artículos 16 y 17 de la Ley Modelo, los cuales se enuncian a continuación: indicación de las marcas, el número, la cantidad o el peso de las mercancías; declaración de la índole o el valor de las mercancías; emisión de un recibo por las mercancías; confirmación de haberse completado la carga de las mercancías; notificación a alguna persona de las cláusulas y condiciones del contrato; comunicación de instrucciones al portador; reclamación de la entrega de las mercancías; autorización para proceder a la entrega de las mercancías; notificación de la pérdida de las mercancías o de los daños que hayan sufrido; cualquier otra notificación o declaración relativas al cumplimiento del contrato; promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega; concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías; y, adquisición o transferencia de derechos y obligaciones con arreglo al contrato), y documentos de transporte.

Estos numerales enuncian ciertas disposiciones aplicables a los documentos de transporte no negociables, a la transferencia de derechos en las mercancías por medio de un conocimiento de embarque negociable o transferible y, en general, al transporte de mercancías por otros medios, tales como al transporte aéreo y al transporte por carretera y ferrocarril.

Especialmente, esta disposición establece en la materia que en los casos en que la ley requiera que alguno de los actos relacionados con los contratos de transporte de mercancías, se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

En nuestro país, aún no ha sido abordado a fondo el tema de comercio electrónico en la Ley de Navegación y Comercio Marítimo; sin embargo, ya existe un adelanto en dicho ordenamiento, al referirse en su numeral 262, que cuando en los Incoterms se haga referencia a la posibilidad de sustituir un conocimiento de embarque o cualquier otro documento de transporte similar por un mensaje de intercambio electrónico de datos (EDI) equivalente; tal documento será un título de crédito solamente cuando reúna los elementos para considerarse como tal de conformidad con la Ley General de Títulos y Operaciones de Crédito.

Aún falta por establecer en la citada ley marítima, todos y cada uno de los principios establecidos sobre el comercio electrónico en la materia, establecidos en la Ley de la CNUDMI sobre Comercio Electrónico; reto que confío, México puede alcanzar.

2.6. Cuestiones de la fiscalidad en relación con el comercio electrónico.¹⁰⁷

La nueva modalidad de la actividad comercial mediante medios electrónicos, ha motivado a la comunidad internacional a intervenir para abordar las implicaciones fiscales que emergen de la misma. En esa tesitura, han sido debatidas diversas posturas en foros internacionales; asimismo, se han considerado las experiencias del tesoro de Estados Unidos, en virtud de que ésta nación es punta de lanza en materia de fiscalidad del comercio electrónico.

Cabe citar dos de los organismos internacionales más importantes por competencia y por la calidad de sus aportaciones efectuadas en esta materia, a saber: la OCDE (Organización para la Cooperación y Desarrollo Económico), y la Unión Europea.

La OCDE, como organismo internacional de naturaleza consultiva, cuyas recomendaciones carecen de “fuerza” vinculatoria para los Estados miembros, ha

¹⁰⁷ Joan Hortalà i Vallvé, Franco Roccatagliata y Piergiorgio Valente, *La fiscalidad del comercio electrónico*, p.p. 119.

abundado en aspectos legales de la fiscalidad directa e indirecta, y en particular su Comité de Asuntos Fiscales (CFA), están desempeñando estudios de fondo sobre la llamada revolución tecnológica y de las comunicaciones en general del comercio electrónico, en particular, sobre la fiscalidad internacional.

La OCDE ha auspiciado sendas reuniones internacionales en Turku y Ottawa donde se han sentado las bases del futuro acuerdo, a nivel mundial, en materia fiscal sobre comercio electrónico.

En 1997, la OCDE organizó en Turku (Finlandia) una conferencia informal, con representantes del sector público y privado, para efecto de tratar las repercusiones sobre la política fiscal y la administración tributaria derivadas del comercio electrónico.

Como resultados de este encuentro se subrayan los siguientes puntos de acuerdo, además de aquéllos en los que se requiere un mayor debate, a saber:

- La fiscalidad no puede convertirse en un obstáculo que dificulte el desarrollo del comercio electrónico, aunque simultáneamente, el comercio electrónico no debe favorecer la inaplicación de las normas tributarias.
- Los gobiernos deberán estudiar las propuestas que garanticen la neutralidad de las operaciones económicas y aseguren un adecuado reparto de las bases tributarias evitando la doble imposición así como la evasión.
- Los gobiernos debe explotar al máximo los actuales instrumentos tributarios antes de plantearse la posibilidad de adoptar nuevos modos de someter a imposición estas operaciones.
- No parece necesario el establecimiento del bit-tax (forma de tributación basada en la interactividad y en la intensidad telemática de las transmisiones).

- La nueva sociedad de la información permitirá también a las Administraciones fiscales mejorar en eficiencia el manejo de mayores volúmenes de información de las actividades desarrolladas por sus contribuyentes.
- En materia de IVA, los participantes convinieron que el tipo de operaciones donde la interacción entre comercio electrónico e IVA pueden plantear problemas es bastante reducido, si bien el volumen de rentas implicadas puede ser potencialmente importante.
- Hubo consenso en cuanto a que la cooperación internacional es el único modo de alcanzar resultados satisfactorios.

Las características del IVA radica en que incide en el consumo, ya que es el consumidor quien soporta el peso de la carga fiscal. El control y la recaudación del IVA se efectúan por el proveedor de bienes y servicios, quien generalmente no resulta afectado por este gravamen. Las actividades económico-financieras de producción, distribución, importación y exportación de bienes y servicios tienen como objetivo final el consumo privado y el público, nacional y extranjero; por lo que, el IVA como gravamen al consumo incide en estas actividades gravándolas o liberándolas del gravamen, según sea el caso.¹⁰⁸

De los que se requiere un mayor debate, se encuentran los siguientes puntos:

- Desde el punto de vista temporal, las Administraciones fiscales se muestran preocupadas por el importante crecimiento de las operaciones realizadas a través de la red, sin que los sistemas tributarios hayan podido adaptarse suficiente y adecuadamente; por lo que, demandan cierta urgencia en la adopción de decisiones; por el contrario, el sector empresa indicó que las modificaciones tributarias

¹⁰⁸ Sánchez Miranda, Arnulfo, *Estrategias Financieras de los Impuestos*, Sistemas de Información Contable y Administrativa Computarizados, Sociedad Anónima de Capital Variable, Primera edición, México, 2000, pág. 225.

deben efectuarse de modo paulatino y sin bruscos cambios de rumbo; acordado así, la necesidad de planificar los cambios que resulten necesarios, no de manera apresurada.

- Hubo acuerdo en cuanto a la dimensión del comercio electrónico actual y potencial, en el cual se disertó que no basta con los datos acerca de la importancia relativa del comercio electrónico en relación con el comercio total, sino que son también necesarios otros indicadores como el índice de penetración potencial de Internet.
- La necesidad de adaptar las definiciones de residencia, cánones, etcétera, en los tratados de doble imposición, las medidas anti-abuso y demás legislación fiscal.
- Los datos que deben ser accesibles a las Administraciones tributarias.

Derivado de lo anterior, los gobiernos solicitaron a la OCDE, el estudio de diversas cuestiones, como:

- ⊕ Cómo organizar la Administración tributaria en las áreas afectadas por el comercio electrónico.
- ⊕ En qué modo puede emplearse el intercambio de información a fin de evitar la evasión fiscal.
- ⊕ De qué forma deben adaptarse los Convenios de doble imposición.
- ⊕ De modo conjunto con la Unión Europea, estudiar la fiscalidad de estas operaciones en el ámbito de la imposición indirecta, en particular del IVA.

Las instituciones de la Unión Europea y la Comisión en particular, se han avocado particularmente en la fiscalidad indirecta. Un grupo de expertos hizo seguir un informe en abril de 1997, el cual, se centra en las repercusiones a nivel social de la evolución tecnológica, y aborda una serie de problemas a los que deberán hacer frente los políticos cuando la sociedad de la información se haya desarrollado por completo

en Europa. El documento además propone un modelo europeo de sociedad de la información, basado en un carácter social, y recomienda la búsqueda de un método que permita una distribución equitativa de los beneficios que derivarán de la implantación de la sociedad de la información. Asimismo, este grupo propuso a la Comisión estudiar la posibilidad de adoptar una bit-tax.

El bit-tax, es el “impuesto sobre el bit”; el bit es la contracción de la expresión “binary digit” (cifra binaria); esto es, la unidad de medida de los datos en informática. La velocidad de la transmisión de la información se mide en bits en segundo.

Esta proposición al bit-tax, ha sido discutida, principalmente en virtud de que la aplicación de este impuesto provocaría un aumento de los precios para los usuarios de la red que podría disuadirles de utilizar esta tecnología, en beneficio de otras formas tradicionales de transmisión de la información; esto podría justificarse –como algunos autores lo ha indicado-, en el caso de que la elasticidad de la demanda para los servicios de la red fuera igual o cercana a cero; lo que no acontece en la actualidad.

La Unión Europea ha empezado a formular una serie de directrices políticas sobre el comercio electrónico, bajo la premisa de promover el desarrollo de un mercado interior de servicios electrónicos y salvaguardar el interés público; asimismo, ha propuesto lanzar un debate internacional sobre la materia, cuyos puntos a destacar se encuentran:

I). Establecer un marco para la cooperación internacional, y suprimir obstáculos al mercado electrónico mundial.

II). La no conveniencia de la creación de una entidad supervisora a escala internacional, ni de establecimiento de una normativa vinculante que no representen el resultado de una adecuada mediación entre las exigencias de las distintas partes implicadas en las nuevas tecnologías.

Por su parte, Estados Unidos de América, ha manifestado por conducto del Departamento del Tesoro, su preocupación en relación con las implicaciones del

comercio electrónico en la fiscalidad; los problemas prioritarios, reales y potenciales, mismos que han sido recogidos en el Informe del Office of Tax Policy del Departamento del Tesoro, “Selected Policy Implications of Global Electronic Commerce. El informe expone el riesgo de conflicto entre las Administraciones fiscales y de doble imposición en las operaciones transfronterizas realizadas a través de las modernas tecnologías de información. Asimismo, esta nación ha propuesto en su documento “Framework for Global Electronic Commerce”, que el mercado cibernético sea considerado zona franca o libre de imposición, y ponen de manifiesto las autoridades norteamericanas, que solo obtendrían la exención, las operaciones on-line o totalmente electrónicas.

Es importante establecer, que Estados Unidos como punta de lanza en la presente materia, defiende el principio de neutralidad, el cual, radica en el hecho de que a los productos o servicios solicitados y suministrados a través de Internet, no se aplique un régimen tributario distinto.

El fin que se busca, es llegar a un equilibrio entre la importancia de recaudación que tiene el Estado, y la no obstaculización al desarrollo del comercio electrónico; por lo que, es necesario llegar a acuerdos internacionales, bajo la premisa: “en la multitud de consejeros, hay seguridad”.

3. El comercio electrónico en México, y derecho comparado.

Según datos estadísticos, tenemos que en México, 2% de su población pertenece a la clase alta, cerca del 18% pertenece a la clase media, alrededor de 50% está inserta en la clase media, y 30% restante forma la clase denominada popular.¹⁰⁹

En 2004, según estudios de SIGMA Consultores, las clases altas y media son quienes poseen más satisfactores en lo que respecta a comunicación en el hogar. La totalidad de los hogares de la clase alta y 92% de la clase media cuenta con teléfono,

¹⁰⁹ Cavazos Arroyo, Judith y Reyes Guerrero, Soraya, *Comercio electrónico: un enfoque de modelos de negocio*. editorial Grupo Editorial Patria, Sociedad Anónima de Capital Variable, Primera reimpresión, México, 2008, p.p. 80.

contra 46% de la clase baja y 1% de la clase popular. Un 99% de la clase alta cuenta con computadora en el hogar y 6 de cada 100 hogares de nivel medio la poseen; a diferencia de las clases bajas con un 17%, y popular 3%.¹¹⁰

Se encontró, que 3% de la clase alta, 3% de la clase media-alta y 1% de la clase media-baja compraban o vendían en línea. Se expuso que el 18% de los internautas compró o pago en línea algún producto, sobre una base estimada por esta Asociación, de 15,000,000 de mexicanos en línea.¹¹¹

Por otro lado, la Asociación Mexicana de Internet (AMIPCI), según estudios mostró que la mayor parte de los usuarios de la red utilizan una conexión de banda ancha; la edad de quienes más se conectan a Internet oscila entre los 13 y 34 años.¹¹²

Actualmente, más de 15,000 empresas mexicanas utilizan los medios de transacción electrónicos, como lo es el EDI (intercambio electrónicos de datos), e Internet.¹¹³

Según el INEGI, en últimas encuestas (2010); 38.9 millones de personas son usuarios de una computadora y 32.8 millones tienen acceso a Internet. Existen 8.44 millones de hogares equipados con computadora, lo que representa un 29.8% del total de hogares en el país. Entidades como el Distrito Federal, Nuevo León, Sonora y Baja California, cuatro de cada diez hogares cuentan con computadora, que significa un promedio de 43.4%; mientras que Chiapas, Guerrero y Oaxaca sólo uno de cada diez hogares tiene acceso a una computadora, en un promedio de 14 por ciento. En cuanto a conectividad, 6.3 millones de hogares cuentan con conexión a Internet, lo cual, representa 22.2% del total en México. La encuesta permitió identificar entre los diversos usos que se le dan a la computadora: labores escolares (53.4%); actividades vinculadas con la comunicación (44%); entretenimiento (37.9%), y trabajo (32.2 por ciento). La encuesta levantada arrojó que el 5% de los usuarios de Internet (un total

¹¹⁰ Ídem.

¹¹¹ Cavazos Arroyo, Judith y Reyes Guerrero, Soraya, *Comercio electrónico: un enfoque de modelos de negocio*. editorial Grupo Editorial Patria, Sociedad Anónima de Capital Variable, Primera reimpresión, México, 2008, p.p. 81.

¹¹² Ídem.

¹¹³ Ídem.

de un millón 629 mil 150 personas), declaró haber comprado o pagado algo en línea.¹¹⁴

No obstante, este crecimiento en el uso de esta tecnología de información y comunicación, se estima que el número de internautas aumentará, en la medida de la apertura que a través de Internet se ha dado a la disposición de información, así como a la adquisición de bienes o servicios.

3.1. Regulación del comercio electrónico en México¹¹⁵

Como antecedentes legislativos en esta materia se citan algunos, como el **Código de Comercio de 1884**, que establecía la correspondencia telegráfica. El **Código Civil de 1928**, que admitió la manifestación de la voluntad por teléfono; las **Reglas y Usos Uniformes sobre Créditos Documentarios**, expedidas por la Cámara Internacional de Comercio, que reconocían la equivalencia funcional entre el papel y el mensaje contenido en télex, medio por el cual se obligaba a los bancos notificar al beneficiario de los créditos documentarios la existencia de uno a su favor; la **Ley Federal de Protección al Consumidor**, anterior a las reformas del 2000, establecía las ventas a distancia (Telemarketing); la **Ley de Navegación y Comercio Marítimos**, se refería a las compraventas fuera de plaza o contra documentos, por ejemplo, la venta CIF (costo, seguro, fletes), reconocidas por los Incoterms; las **leyes bancarias de 1990** y la **Ley Reglamentaria del Servicio Público de Banca y Crédito de 1995**, en las que se había admitido la validez de la información contenida en sistemas telemáticos, considerando que los negativos originales de cámara de microfilmes hechos de libros, registros y documentos por las instituciones bancarias tiene el mismo valor probatorio que los libros, registros y documentos microfilmados; disposición que se mantiene vigente en la **Ley de Instituciones de Crédito**, así como en la **Ley de Organizaciones Auxiliares de Crédito**, y **Ley del Mercado de Valores**.

¹¹⁴ www.inegi.org.mx

¹¹⁵ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, *La firma electrónica avanzada*, Oxford University Press México, Sociedad Anónima de Capital Variable, México, 2007, p.p. 37-53.

México, en la década de 1990, enmendó y adoptó sus leyes para promover el comercio electrónico; ello, en virtud de las operaciones que de manera significativa comenzaban a practicarse. A mediados de los noventa se reconoce la equivalencia funcional de la información contenida en papel con la información contenida en ciertos archivos telemáticos y electrónicos o de tecnologías similares, facilitados con la comunicación y envío de información a través de EDI, fax, Internet, correo electrónico y otros medios electrónicos.

Sin embargo fue hasta 1999, cuando México toma la decisión legislativa de analizar la necesidad de regular el comercio electrónico, considerando la propuesta de la CNUDMI en su Ley Modelo sobre Comercio Electrónico; lo cual, dio lugar a que en agosto de ese año, se formara un Grupo Impulsor del Comercio Electrónico (GICE) constituido por diversas organizaciones como la Asociación de Banqueros de México (ABM), la Asociación Mexicana de Estándares para el Comercio Electrónico (AMECE), y la Asociación Mexicana de la Industria de Tecnologías de Información (AMITI).

En diciembre de 1999 se presentó una segunda iniciativa ante la Cámara de Diputados, en la cual se proponían reformas a diversas leyes, fundamentalmente al Código de Comercio, para incorporar dentro del Libro segundo relativo al comercio terrestre, un título II denominado “Del comercio electrónico”.

El 22 de marzo de 2000, se presentó una nueva iniciativa de reformas complementarias. Como objetivos de estas reformas, se destacan: el reconocimiento de la validez jurídica del contrato electrónico; la posibilidad de la exigibilidad judicial de los contratos realizados a través de medios electrónicos; medios probatorios del contrato electrónico y valoración de la prueba en juicio; y, la protección a los consumidores.

Así, el 29 de abril de 2000, se aprobaron reformas al Código de Comercio, al Código Civil Federal, a la Ley Federal de Protección al Consumidor y al Código

Federal de Procedimientos Civiles, mismas que entraron en vigor a los nueve días de su publicación en el Diario Oficial de la Federación de 29 de mayo de ese año.

Con estas reformas, en el **Código de Comercio** se añadió un título especial, en el que se reestablecen algunos de los artículos anteriormente derogados, dentro del Libro segundo “Del comercio en general”, en el Título Segundo “Del comercio electrónico”, considerando la necesidad de regular de manera específica la contratación a distancia o aquella en que las partes no están físicamente presentes, reconocer dichas operaciones y dar valor probatorio al uso de los medios electrónicos en los procesos administrativos y judiciales, sin que pueda quedar al arbitrio del juez considerar su validez probatoria.

Dichas reformas se adoptaron parcialmente, pues se omitieron algunos aspectos relativos a las firmas electrónicas, lo que representó inseguridad jurídica para acudir a los tribunales y exigir legítimamente el cumplimiento de las obligaciones derivadas de un contrato celebrado por Internet, pues originaba la inobservación de las características de confidencialidad, confiabilidad, seguridad, secrecía y autoría de la información. Asimismo, no había certeza para enterar y pagar impuestos federales por medios electrónicos, tal y como lo disponían algunos ordenamientos legales en el año 2000.

Ello, representó la necesidad de una reforma al citado capítulo relativo al comercio electrónico (además de reformas al Código Fiscal de la Federación y otras disposiciones de carácter administrativo), para efecto de incluir en el Código de Comercio, tanto los principios contenidos en la Ley Modelo de la CNUDMI sobre Comercio Electrónico, así como de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas. Dichas reformas fueron publicadas el 29 de agosto de 2003, en el Diario Oficial de la Federación, donde se materializa el reconocimiento de la firma electrónica, y su respaldo a través de las instituciones certificadoras.

Entre otras reformas publicadas en el año 2000 al Código de Comercio, se encuentran las referentes al *Registro de Comercio*, publicadas en 29 de mayo de ese

año, en el Diario Oficial de la Federación; en las cuales se establece que el Registro Público de Comercio, operará con un programa informático y con una base de datos central interconectada con las bases de datos de sus oficinas ubicadas en las entidades federativas. Mediante dicho programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral.

En esta misma fecha, se publicaron reformas relativas al archivo mercantil, en donde se crea el *archivo mercantil electrónico*; derivado de la obligación que tienen los comerciantes a conservar por un plazo mínimo de diez años los originales de los mensajes de datos. La Secretaría de Comercio y Fomento Industrial, hoy Secretaría de Economía, es la encargada de emitir la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de dichos documentos electrónicos.

Luego, el 27 de agosto de 2009, se publicaron en el Diario Oficial de la Federación, diversas adiciones al Código de Comercio, relativas a las *garantías mobiliarias*, en lo referente al procedimiento de su inscripción en el Registro Público del Comercio. Se constituyó el Registro Único de Garantías Mobiliarias, donde se inscriben las garantías referidas, con lo que se dará publicidad de las mismas para los efectos que establezcan éste u otros ordenamientos jurídicos, y cuya operación, se lleva por medios digitales, mediante el programa informático establecido por la Secretaría de Economía y en una base de datos nacional.

Respecto a las reformas y adiciones al **Código Civil Federal**, se centraron en el reconocimiento a la celebración de actos jurídicos a través de los medios electrónicos, ópticos o de cualquier otra tecnología, añadiéndose los medios tecnológicos como medio idóneo para expresar el consentimiento, estableciéndose una equivalencia funcional entre el consentimiento expresado por medios tecnológicos o la firma autógrafa; siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta.

En el **Código Federal de Procedimientos Civiles**, se reconoce como prueba la información contenida en los medios electrónicos, ópticos o en cualquiera otra tecnología, y da una serie de reglas para su valoración por parte del juzgador, como la fiabilidad del método para generar, comunicar, recibir o archivar la información, su atribución a las personas obligadas y la posibilidad de acceder a ella en ulteriores consultas; además, de acreditarse que dicha información se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

Asimismo, resaltan las reformas al **Código Fiscal de la Federación**, publicadas en el Diario Oficial de la Federación de 5 de enero de 2004, incorporadas en el Título Primero, del Capítulo segundo, denominado “De los medios electrónicos”; donde se reconoce no sólo la validez, sino la obligación de utilizar mensajes de datos y firma electrónica en las promociones, avisos, documentos de los contribuyentes y de las autoridades fiscales, e incluso la realización de subastas electrónicas de bienes embargados a los contribuyentes.

Con el propósito de adecuar la base legal que garantiza los derechos de los consumidores en el ámbito electrónico, se reformó la **Ley Federal de Protección al Consumidor**, y se adicionó el Capítulo VIII bis “De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología”, publicado en el Diario Oficial de la Federación el 29 de mayo de 2000, en cuyo artículo 76 bis, se contienen disposiciones relativas a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

En 2004, se reformó el artículo 1º, fracción VIII, de la ley en comento, el cual, señala como uno de los principios básicos en las relaciones de consumo, la real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología y la

adecuada utilización de los datos aportados. En esta misma anualidad, se adicionó al artículo 10, que los proveedores no podrán prestar servicios adicionales a los originalmente contratados que no hubieren sido solicitados o aceptados expresamente, por escrito o por vía electrónica, por el consumidor.

Otra reforma a este ordenamiento, fue la relativa a la regulación de la publicidad basura (Spam) y no deseada de los medios electrónicos de los consumidores, quienes pueden exigir a los proveedores se abstengan de usar información sobre los consumidores, así como de ofrecer bienes o servicios en su dirección electrónica; así lo prevén los artículos 17 y 127 de dicha ley.

Asimismo, se reformó el artículo 86 bis, del ordenamiento multicitado, para indicar que en los contratos de adhesión de prestación de servicios, deben incluirse por escrito o por vía electrónica los servicios adicionales, especiales, o conexos, que pueda solicitar el consumidor de forma opcional por conducto y medio del servicio básico.

De igual forma, se le da nuevas atribuciones a la Procuraduría Federal del Consumidor, entre las cuales se encuentran, promover en coordinación con la Secretaría de Economía, la formulación, difusión y uso de códigos de ética, por parte de proveedores, que incorporen los principios previstos por la propia ley en mención, respecto de las transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

Otro cambio novedoso, son las denuncias y las quejas ante la Procuraduría Federal del Consumidor, que pueden hacerse por vía electrónica o por cualquier otro medio (artículos 97 y 99, del ordenamiento en cita). En ese sentido, se establece que las notificaciones personales que realice la Procuraduría, deberán realizarse por notificador o por correo certificado con acuse de recibo del propio notificado o por cualquier otro medio fehaciente autorizado legalmente o por el destinatario, siempre y cuando éste manifieste por escrito su consentimiento. Asimismo, se establece que la documentación que sea remitida por una unidad administrativa de la Procuraduría vía

electrónica, fax o por cualquier otro medio idóneo a otra unidad de la misma para efectos de su notificación, tendrá plena validez siempre que la unidad receptora hubiere confirmado la clave de identificación del servidor público que remite la documentación y que ésta se conserve íntegra, inalterada y accesible para su consulta; ello, previsto en el artículo 104 del código multicitado.

Por su parte, en la **Ley del Servicio de Tesorería de la Federación**, el 29 mayo de 1998, fue publicado en el Diario Oficial de la Federación, una reforma al artículo 14-Bis, que indica que la Tesorería estará facultada para celebrar las operaciones y prestar los servicios a que se refiere la presente Ley, mediante la utilización de documentos escritos con la correspondiente firma autógrafa del servidor público competente, o bien, a través de equipos o sistemas automatizados, para lo cual, en sustitución de la firma autógrafa, se emplearán medios de identificación electrónica.

El 28 de mayo de 2009, se publicaron en el Diario Oficial de la Federación, reformas al artículo 28, de la **Ley de Obras Públicas y Servicios Relacionados con las Mismas**, en lo relativo a las licitaciones públicas con la utilización de medios electrónicos, y en las cuales se establece que en estas se podrán utilizar medios electrónicos, conforme a las disposiciones administrativas que emita la Secretaría de la Función Pública; lo anterior, sin perjuicio de que los licitantes puedan optar por presentar sus proposiciones por escrito durante el acto de presentación y apertura de proposiciones, además de que las proposiciones presentadas deberán ser firmadas autógrafamente por los licitantes o sus apoderados. En el caso de que éstas sean enviadas a través de medios remotos de comunicación electrónica, en sustitución de la firma autógrafa, se emplearán medios de identificación electrónica, los cuales producirán los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

Asimismo, se reformó la **Ley Federal de Procedimiento Administrativo**, en su artículo 35, a efecto de establecer que las notificaciones, citatorios, emplazamientos, requerimientos, solicitud de informes o documentos y las

resoluciones administrativas definitivas también podrán realizarse: mediante telefax, medios de comunicación electrónica o cualquier otro medio, cuando así lo haya aceptado expresamente el promovente y siempre que pueda comprobarse fehacientemente la recepción de los mismos, y en tratándose de actos distintos a los señalados anteriormente, las notificaciones podrán realizarse por correo ordinario, mensajería, telegrama o, previa solicitud por escrito del interesado, a través de telefax, medios de comunicación electrónica u otro medio similar.

En este ordenamiento, también se adicionó el artículo 69-C, que indica que los titulares de las dependencias u órganos administrativos desconcentrados y directores generales de los organismos descentralizados de la administración pública federal podrán, mediante acuerdos generales publicados en el Diario Oficial de la Federación, establecer plazos de respuesta menores dentro de los máximos previstos en leyes o reglamentos y no exigir la presentación de datos y documentos previstos en las disposiciones mencionadas, cuando puedan obtener por otra vía la información correspondiente. Esta reforma establece la posibilidad de que los particulares puedan presentar promociones, además de por escrito, a través de medios de comunicación electrónica en las etapas de las propias dependencias y organismos que así lo determinen mediante reglas de carácter general publicado en el Diario Oficial de la Federación.

En ese orden, el 11 de junio de 2002, es publicada en el Diario Oficial de la Federación, la **Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental**, encargada de proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.

Y, en 2004 se crea **Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación**, publicado el 19 de julio de la citada anualidad; el cual, tiene por objeto establecer las normas reglamentarias a las que deben sujetarse los Prestadores de Servicios de Certificación en materia de firma electrónica y expedición de certificados para actos de comercio.

3.2. Situación actual del comercio electrónico en España.

En 1999, la @ECE (**Asociación Española de Comercio Electrónico**), realizó un estudio en relación con el comercio electrónico en España, en el que sobresalen los siguientes datos y estimaciones:¹¹⁶

- En 1998, las empresas españolas generaron ingresos por valor de 3.400 millones de pesetas, cifra que supone un crecimiento del 425% con respecto a 1997, año en que el comercio electrónico alcanzó los 800 millones.
- El 64% de las empresas, entrevistadas manifestaron tener acceso al correo electrónico.
- El 66% de las empresas disponen de acceso a la World Wide Web para navegar.
- El 16% de las empresas españolas disponen de su página web.
- El 56% del total de las empresas españolas ofrecen sus servicios a través de Internet.
- El 9% total de las empresas que se dirigen al consumidor final afirma estar haciendo comercio electrónico, lo que significa que el 56,25% de las empresas a través de Internet están ofreciendo sus productos y servicios.

Asimismo, la @ECE elaboró un estudio, en el cual establece dos consecuencias de esta modalidad de comercio electrónico:¹¹⁷

- 1) Las solicitudes de información a través de Internet tienen un índice de conversión a ventas (fuera de Internet) más elevado que ningún otro

¹¹⁶ Joan Hortalà i Vallvé, Franco Roccatagliata y Piergiorgio Valente, *La fiscalidad del comercio electrónico*, p.p. 30.

¹¹⁷ Joan Hortalà i Vallvé, Franco Roccatagliata y Piergiorgio Valente, *La fiscalidad del comercio electrónico*, p.p. 32.

medio de comunicación.

- 2) Las empresas que hacen comercio electrónico con productos o servicios que requieren una inversión superior a las 25.000 pesetas, suelen ir seguidas o precedidas de una llamada telefónica. Por lo que, estiman que esta llamada denota todavía relativa inseguridad del canal para los usuarios, y distorsiona las cifras ya que las ventas suelen cerrarse fuera de Internet y las empresas no las cuantifican como ingresos precedentes del comercio electrónico.

Concluye la citada asociación, que la distribución por sectores de Internet refleja una mayor implicación del sector informático, seguido de la distribución, servicios y transporte. Y expone, que las razones alegadas para llevar a cabo la actividad de comercio electrónico, responden mayoritariamente a la mejora del servicio al cliente seguido de la ampliación geográfica del mercadeo; la agilización de la venta y entrega del producto o la obtención de niveles de competitividad más altos. En sentido contrario, señala que las razones que se aducen para no desarrollar una actividad de comercio electrónico, se centran en la inadecuación del producto al canal y desconocimiento tecnológico.

Como productos objeto del comercio electrónico en España, se desprenden los siguientes, en orden de importancia: reserva de viajes, reservas de alojamiento, información financiera, hardware, ropa, software, libros, suscripciones, electrónica, transporte de mercancías, seguros, productos sanitarios, mensajería, automóviles, inmobiliaria. Entre los productos que mayormente se han rechazado a la compra en Internet, se encuentran los automóviles e inmuebles.

Como bien lo refiere los autores Joan Hortalà i Vallvé, Franco Roccatagliata y Piergiorgio Valente, con ello se confirma la tendencia de que los internautas españoles prefieren comprar productos estándar como libros, música y software, donde la decisión de compra se hace sobre el conocimiento de un producto “simple”, y al momento de comprar un automóvil o un inmueble, la decisión es más compleja, pues son bienes que requieren un conocimiento en detalle.

En cuanto al precio medio, se expone que casi el 90% de las compras realizadas por los internautas españoles no sobrepasan las 25.000 pesetas. Asimismo, por lo que hace a los sistemas de pago utilizados, se observan las transferencias bancarias y la domicialización bancaria, seguidos por el contra reembolso y las tarjetas de crédito.

Por su parte, cabe resaltar las estadísticas que hace la **Comisión del Mercado de las Telecomunicaciones**¹¹⁸, quien es la Autoridad Nacional de Regulación española, organismo público regulador independiente de los mercados nacionales de comunicaciones electrónicas y de servicios audiovisuales en España, cuyo principal objetivo es el establecimiento y supervisión de las obligaciones específicas que hayan de cumplir los operadores en los mercados de telecomunicaciones y el fomento de la competencia en los mercados de los servicios audiovisuales, así como la resolución de conflictos entre los operadores.

Dicha Comisión, como órgano arbitral, elaboró un informe sobre el comercio electrónico a través de algunas entidades de medios de pago, relativos al cuarto trimestre de 2009; de los que caben destacar lo siguientes:

a) El volumen de negocio de las transacciones con origen en España y dirigidas hacia el exterior fue de 722 millones de euros, con 11 millones de operaciones. El importe de las transacciones realizadas desde el exterior y dirigidas a sitios web españoles fue de 155,6 millones de euros, con 1,3 millones de operaciones.

b) La cifra de negocio del comercio electrónico generado en España y dirigido a puntos de venta virtuales dentro del país fue de 696,7 millones de euros, con 9,8 millones de operaciones.

c) El comercio electrónico en España alcanzó un volumen de negocio de 1.574,2 millones de euros, con un total de 22,1 millones de operaciones.

¹¹⁸ www.cmt.es

d) Las ramas de actividad con mayor peso en las cifras de ingresos fue el transporte aéreo (14%), las agencias de viajes y operadores turísticos (10,3%), el marketing directo (9,8%), el transporte terrestre de viajeros (6,8%), los juegos de azar y apuestas (6,1%), los espectáculos artísticos, deportivos y recreativos (5,7%), los servicios legales, contabilidad y gestión (4,6%), la administración pública, impuestos y seguridad social (3,3%), los ordenadores y programas informáticos (2,9%), y, por último, los electrodomésticos, radio, televisión y sonido (2,6%).

e) Se ha evaluado el volumen de negocio de comercio electrónico desde España con el exterior de forma agregada y se ha distribuido por ramas de actividad, obteniendo como resultado que de las diez ramas que obtienen un mayor porcentaje del volumen total, los juegos de azar y apuestas fueron la rama de actividad más importante (10,4%), seguido por los servicios legales, contabilidad y gestión (9,9%), el transporte aéreo (9,5%), el marketing directo (8,8%), los ordenadores y programas informáticos (5,4%), y las agencias de viajes y operadores turísticos (4,5%). A continuación está la publicidad (2,5%), y los electrodomésticos, radio, televisión y sonido (2,5%). En la parte inferior del ranking se situaron los teléfonos públicos y tarjetas telefónicas (2,2%) y, por último, los hoteles, apartamentos y camping (1,9%) La Unión Europea, como viene ocurriendo en todos los trimestres, fue el destino preferido para realizar compras en el extranjero.

f) Respecto a las ramas de actividad más favorecidas en términos de volumen de negocio, el sector turístico (que comprende el transporte aéreo, las agencias de viaje y operadores turísticos y los hoteles, apartamentos y camping y el transporte terrestre de viajeros) supuso el 68,9% de los ingresos. En orden de importancia por ingresos, le siguieron el marketing directo (7,2%), la educación (3,5%) y los espectáculos artísticos, deportivos y recreativos (2,3%). Cerraron la lista de ramas de actividad más importantes la publicidad (2,2%), los electrodomésticos, radio, televisión y sonido (2%) y la administración pública, impuestos y seguridad social (1,6%).

g) Los ingresos del comercio electrónico a través de las entidades de medio de pago que se realizaron dentro de España alcanzaron la cifra de 696,7 millones de euros, el 44,3% del total del volumen de negocio y un 34% más que en el mismo periodo del año precedente. El sector turístico, considerado como la agregación del transporte aéreo y el transporte terrestre de viajeros y las agencias de viaje y operadores turísticos (16,3%, 13,8% y 10,7%, respectivamente), constituyó el 40,8% de los ingresos del comercio electrónico dentro de España. También resultaron relevantes el marketing directo (11,5%), los espectáculos artísticos, deportivos y recreativos (11,4%) y la administración pública, impuestos y seguridad social (7%). Cerraron la lista los artículos de regalo (3%), los electrodomésticos, radio, televisión y sonido (2,9%), y por último los juegos de azar y apuestas (2,8%) y la educación (2,6%).

Asimismo, cabe mencionar la *Asociación Española de Comercio Electrónico*¹¹⁹, surgida en mayo de 1998; la cual se fusionó en 2005, con la Asociación Española de Marketing Relacional, formando así AECEM-FECEMD. En la actualidad, AECEM-FECEMD representa a más de 200 compañías cuya actividad está relacionada con el comercio electrónico y/o con el marketing relacional, y pretende ser una referencia frente a las instituciones gubernamentales y legislativas, en materia de comercio electrónico y en todo aquello que afecte al marketing relacional, directo e interactivo.

Esta Asociación, junto con Marketing Relacional (AECEM), con el apoyo de Plan Avanza Gobierno de España. Ministerio de Industria, Turismo y Comercio, publicó el "Libro Blanco del Comercio Electrónico", con el efecto de tener un manual práctico de utilidad para quienes estén o quieran estar en Internet para vender sus productos o servicios y convertir el canal on-line en una vía de desarrollo y fuente de beneficio.

Dicho trabajo reúne todos los datos cuantitativos (estadísticas, análisis y proyecciones), así como ejemplos, referencias y herramientas de utilidad para cualquier empresa que esté o quiera estar presente en comercio electrónico.

¹¹⁹ www.aecem.org

Asimismo, se pueden encontrar, la visión de profesionales del sector que han vivido y viven de forma directa y personal, los éxitos y dificultades de la venta on-line en todas sus facetas.

En la citada obra, se remarca la importancia de las empresas de estar en Internet, y se establecen estadísticas de acuerdo con los últimos datos procedentes del Estudio B2C publicado por ONTSI (Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información), en el cual se advierte que sólo en España se cuenta con más de 23 millones de internautas habituales de los cuales casi 9 millones compran en Internet de forma frecuente.

De lo que la propia Asociación, concluye que todavía hoy el mercado de venta por Internet en España es reducido, en comparación con otros países de Europa como Reino Unido, Alemania o los países nórdicos y sobre todo en comparación con Estados Unidos, donde el mercado alcanzó en 2007 nada menos que los 175 billones de dólares según los datos aportados por Forrester y Jupiter Research.

Por su parte, se encuentra el *Instituto Nacional de Estadística*¹²⁰, creada en la Ley de 31 de diciembre de 1945 (publicada en el BOE del 3 de enero de 1946, que tiene como misión la elaboración y perfeccionamiento de las estadísticas demográficas, económicas y sociales ya existentes, la creación de otras nuevas y la coordinación con los servicios estadísticos de las áreas provinciales y municipales en España. Además de regular la coordinación entre otros servicios estadísticos como el Servicio Sindical de Estadística, la Ley crea el Consejo Superior de Estadística. El Instituto Nacional de Estadística se organiza en Servicios Centrales, Delegaciones provinciales y Delegaciones en los Ministerios.

Este instituto, hizo una encuesta el 15 de octubre de 2008, sobre el uso de TIC y del Comercio Electrónico en las empresas 2007/08, en colaboración con el Instituto de Estadística de Navarra (IEN), quien ha formalizado un convenio de colaboración con la Fundación Centro Tecnológico de la Información y Comunicación (CTIC) del Principado de Asturias.

¹²⁰ www.ine.es

Es una encuesta integrada en los planes de estadísticas de la Unión Europea para cuantificar la Sociedad de la Información. Se rige por el reglamento N° 808/2004 del Parlamento Europeo y del Consejo para la realización de estadísticas sobre la Sociedad de la Información. El objetivo de esta operación estadística es obtener la información necesaria para medir el uso de las Tecnologías de la Información y las Comunicaciones y el Comercio Electrónico en las empresas de los estados miembros y así dar respuesta a los indicadores de comparativa 2010 en lo que se refiere al ámbito empresarial.

En dicha encuesta se destacan los siguientes, a saber:

- El 94,9% de las empresas españolas de 10 ó más asalariados dispone de conexión a internet, de las cuales el 97,1% accede a través de banda ancha.
- El porcentaje de empresas que interactúa a través de internet con las administraciones públicas aumenta cinco puntos respecto al año pasado y alcanza el 67,1%.
- La compra de bienes y servicios a través de comercio electrónico registra un crecimiento interanual del 28,3%.
- El 94,9% de las empresas españolas de 10 ó más asalariados dispone de conexión a internet, según la Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del Comercio Electrónico en las empresas.
- El uso de ordenadores está extendido en la práctica totalidad de las empresas de 10 ó más trabajadores (el 97,8%). Por su parte, el 78,5% tiene instalada una Red de Área Local (LAN) y el 29,2% dispone de una Red de Área Local sin hilos.
- En lo que se refiere a las comunicaciones electrónicas, un 93,3% de empresas dispone de correo electrónico y en un 91,2% está implantada la telefonía móvil.
- De las empresas con conexión a internet, el 57,5% dispone de sitio/página web. En el colectivo formado por las de 250 ó más

asalariados, un 89,2% declara disponer de página web, lo que supone un incremento de más de dos puntos respecto al periodo precedente.

- Un 14,7% de las empresas tienen empleados que realizan teletrabajo, es decir, trabajan fuera de sus locales de forma regular (al menos media jornada semanal), y se conectan a los sistemas TIC de su empresa mediante redes telemáticas externas. Esta cifra supone un incremento interanual del 19,4%.
- Las empresas de Comunidad de Madrid, Cataluña, País Vasco y Comunidad Foral de Navarra utilizan las TIC con mayor intensidad.
- Por comunidades autónomas, las empresas ubicadas en la Comunidad de Madrid, Cataluña, País Vasco y Comunidad Foral de Navarra presentan las mayores intensidades en el uso de las TIC.
- Por el contrario, las empresas de Castilla-La Mancha, de las ciudades autónomas de Ceuta y Melilla, de Extremadura y de Cantabria tienen los menores porcentajes de uso de nuevas tecnologías.
- El 97,1% de las empresas con conexión a internet utiliza banda ancha. Entre las empresas españolas de 10 o más asalariados con conexión a internet, el 97,1% acceden mediante alguna solución de banda ancha. La tecnología más utilizada es la conexión mediante soluciones DSL (con un 94,4%), mientras que el acceso mediante otras conexiones fijas supone un 8,1%.
- La mayoría de las empresas utiliza internet para buscar información (97,2%) y para obtener servicios bancarios y financieros (86,0%).
- Los principales objetivos fueron la descarga de impresos y formularios (63,0%), la obtención de información desde las páginas web de las Administraciones Públicas (62,0%), y el envío de impresos cumplimentados (47,3%).
- Más de la mitad de las empresas con conexión a Internet tienen página web. El 57,5% de las empresas españolas con conexión a Internet dispone de página web.

- Las empresas utilizan su página web principalmente para dar a conocer la empresa y sus productos (un 88,2%) y para facilitar el acceso a catálogos y listas de precios (un 56,9%).
- Una de cada dos empresas utiliza la firma digital en alguna comunicación con agentes externos. De las empresas que hacen uso de la misma, el 91,7% la emplean para relacionarse con la Administración Pública, mientras que el 19,8% la emplean para relacionarse con proveedores y clientes.
- Los servicios de seguridad más empleados por las empresas con conexión a Internet son el software de protección o chequeo de virus (97,1%), los cortafuegos o *firewalls* (76,8%) y los mecanismos de autenticación (68,1%).
- Un 11,2% de las empresas declara haber tenido algún problema de seguridad en los últimos 12 meses.
- El 32,0% de las empresas realizan intercambio automatizado de datos con otros sistemas TIC externos. Los mensajes intercambiados con más frecuencia son el envío de instrucciones de pago a entidades bancarias (72,0%) y el intercambio de información con la Administración Pública (58,8%).
- Una de cada cuatro empresas comparte información electrónicamente con proveedores y clientes sobre la cadena de suministro. El 59,3% de estas empresas comparte información sobre el estado de envíos con sus proveedores y el 45,8% con sus clientes.
- En cuanto a la implantación de sistemas de negocio electrónico, un 23,2% de las empresas declara utilizar herramientas informáticas ERP (Planificación de recursos empresariales) para compartir información electrónicamente entre distintas áreas. Por su parte, un 23,8% dispone de aplicaciones CRM (Administración de la relación con los clientes) para gestionar la información sobre clientes.
- El 11,0% de las empresas realizaron ventas mediante comercio electrónico (a través de Internet u otras redes telemáticas) en 2007. El

volumen de negocio generado por estas ventas alcanzó los 140.975 millones de euros, con un incremento interanual del 11,1%.

- La rama de actividad con mayor porcentaje de empresas (calculado sobre el total de empresas de la rama) que realizaron ventas a través de comercio electrónico fue *Hoteles y camping* (64,0%).
- Las ventas a través de comercio electrónico representaron el 8,3% del total de ventas efectuadas por las empresas españolas. La rama de actividad de *Coquerías, refino de petróleo; química; caucho y materias plásticas* mostró la mayor proporción de ventas por comercio electrónico sobre el total de sus ventas, con un 21,5%.
- El 93,5% de las ventas por comercio electrónico tuvieron como destino las empresas (el denominado business to business, B2B). Por su parte, el porcentaje de ventas a consumidores finales (business to consumer, B2C) fue del 5,5% y las ventas con destino a la Administración Pública (business to Government, B2G) aglutinaron el porcentaje restante.
- Por destino geográfico, el 84,0% de las ventas tuvo como destino a España y el 10,1% a otros países de la Unión Europea.
- El 21,4% de las empresas compra a través de comercio electrónico.
- El 21,4% de las empresas realizaron compras mediante internet u otras redes telemáticas en 2007, lo que supone un aumento interanual del 11,1%. El volumen total de los pedidos de bienes y servicios realizados a través de comercio electrónico registró un incremento del 28,3% y alcanzó los 153.889 millones de euros.
- La rama de actividad que presentó mayor porcentaje de empresas que compran a través de comercio electrónico fue *Actividades informáticas* (59,5%).
- Las compras a través de comercio electrónico representaron el 12,6% de los pedidos totales efectuados por las empresas.
- Los resultados referidos a la población de empresas de menos de 10 asalariados revelan una sostenida tendencia al alza, tanto en las infraestructuras como en el uso de las TIC, aunque aún se observan

notables diferencias respecto a la población de empresas de más de 10 asalariados.

- Así, en enero de 2008 el 64,7% de las empresas de menos de 10 asalariados dispone de ordenadores y el 20,9% tiene instalada una Red de Área Local (LAN).
- En cuanto al uso de Internet, el 53,0% de las empresas pequeñas dispone de acceso a Internet. El 92,3% de las empresas con conexión a Internet acceden mediante alguna solución de banda ancha, con un aumento del 2,2% respecto al período precedente.
- El 49,1% utiliza el correo electrónico, mientras que el porcentaje de empresas con menos de 10 asalariados usuarias de telefonía móvil alcanza el 69,1%.
- En cuanto a la presencia en la Red, el 21,4% de las empresas con conexión a Internet dispone de página web.

Respecto de la legislación sobre comercio electrónico en España, quien forma parte de la Unión Europea, cabe destacar las comunicaciones, Directivas, como otros documentos generales, que están directamente relacionadas como el comercio electrónico. Asimismo, se encuentra la Ley 34/2002 de 11 de julio, “De Servicios de la Sociedad de la Información y de Comercio Electrónico”, la cual tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre comercio electrónico); asimismo, incorpora parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores.¹²¹

3.3. Normativa Colombiana sobre comercio electrónico.

¹²¹ García Más, Francisco Javier, *Comercio y Firma Electrónicos (Análisis Jurídico de los Servicios de la Sociedad de la Información)*, editorial Lex Nova, Sociedad Anónima, Segunda edición, España, 2004, p.p. 258.

La Ley 527 de 1999, es la ley fundamental que rige los aspectos sobre comercio electrónico en Colombia; incorpora los conceptos de la Ley Modelo sobre el Comercio Electrónico, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Esta ley nace de la iniciativa del Gobierno de Colombia de acercarse con los organismos internacionales interesados en el tema, y de los debates e investigaciones realizados por la Comisión Redactora de la Ley colombiana, con la asistencia de representantes de organismos públicos y privados, los cuales concluyeron, que la Ley Modelo propuesta por la Comisión de Naciones Unidas para el Derecho Mercantil, era el instrumento idóneo de referencia para adecuar el derecho interno de ésta nación a las tendencias jurídicas mundiales.¹²²

Como antecedentes de esta ley, cabe señalar que en la década de los noventa, en la cual hubo una creciente tendencia por el uso de tecnologías de la información y la comunicación en la práctica mercantil internacional, algunos foros internacionales iniciaron un estudio específico y detallado de la forma como se desarrollaban estas relaciones con el propósito de que las mismas contaran con la certidumbre necesaria para generar obligaciones y vínculos jurídicos semejantes a los que se daban en un entorno tradicional. Es así, como con base en el seno de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional CNUDMI, el gobierno de Colombia adelantó la labor de adecuación de la propuesta de la CNUDMI a su ordenamiento jurídico interno, dando como resultado que en el año de 1993, el Gobierno Nacional expidiera el Decreto 663 de 1993, en el cual se actualiza el Estatuto Orgánico del Sistema Financiero y se modifica su titulación y numeración, y se establece la viabilidad del uso de los sistemas electrónicos y del intercambio electrónico. Seguido, en 1995, el Congreso de la República expediría la Ley 222, por medio de la cual se reforma el Código de Comercio, y en la que se dispuso la posibilidad de llevar a cabo

¹²² Universidad de los Andes, Facultad de Derecho, Internet, *Comercio Electrónico & Telecomunicaciones*, Legis Editores Sociedad Anónima, Primera edición, Colombia, 2002, p.p. 179.

reuniones de accionistas sin que fuera necesaria su presencia física y simultánea, siempre y cuando se cumplieran los requisitos previstos en la Circular Externa 05/96 de la Superintendencia de Sociedades y, posteriormente, el Gobierno Nacional expediría el Decreto 2150, donde se suprimen y reforman regulaciones, procedimientos o trámites innecesarios, existentes en la Administración Pública, estableciéndose en su artículo 26, que las entidades de la Administración Pública debían habilitar sistemas de transmisión electrónica de datos para que los usuarios envíen o reciban información requerida en sus actuaciones frente a la administración, y que en ningún caso las entidades públicas podrían limitar el uso de tecnologías para el archivo documental por parte de los particulares, sin perjuicio de sus estándares tecnológicos. Más adelante, se establecerían disposiciones relacionadas con la factura electrónica a través de la Ley 223 de 1995, el Decreto 1094 de 1996 y el Concepto de la DIAN No. 40333 de 2000.¹²³

En el año 2000, el Gobierno Nacional expidió el Decreto 1747, en el se establecen los requisitos técnicos y financieros que deben cumplir las entidades de certificación para obtener la autorización por parte de la Superintendencia de Industria y Comercio.¹²⁴

La Ley 527 de 1999, ha sido demandada en dos ocasiones por ser presuntamente contraria, en algunas de sus disposiciones a la Constitución Nacional. En la primera de ellas los demandantes argumentaron que la Ley 527 de 1999 era contraria a la Carta Política en lo referente a las actividades ejercidas por las entidades de certificación, que al considerarse fe pública transgredían las competencias ya asignadas de manera exclusiva a otros actores. La sentencia C- 662-00 resolvió declarando la constitucionalidad de la norma. De la misma manera, la Corte Constitucional declaró la constitucionalidad de la Ley 527 de 1999 a través de la sentencia C-831-01, cuando fue demandado el artículo 6 de la misma, por ser aparentemente contrario a lo dispuesto en la Constitución Nacional.¹²⁵

¹²³ Cfr Universidad de los Andes, Facultad de Derecho, Internet, ob. cit, 176-178.

¹²⁴ www.mincomercio.gov.co

¹²⁵ www.mincomercio.gov.co

Enseguida, se reproduce la Ley 527 de 1999:¹²⁶

“Comercio Electrónico

Legislación Nacional – Colombia

Ley N° 527

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones

El Congreso de Colombia

DECRETA:

PARTE I PARTE GENERAL

CAPITULO I

Disposiciones Generales

Artículo 1. *Ámbito de aplicación.* La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

- a) En las obligaciones contraídas por el Estado colombiano en virtud de Convenios o Tratados internacionales.
- b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

Artículo 2. *Definiciones.* Para los efectos de la presente ley se entenderá por:

a) ***Mensaje de Datos.*** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax

b) ***Comercio electrónico.*** Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de

¹²⁶ Ídem.

operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;

c) Firma Digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

d) Entidad de Certificación. Es aquella persona que, autorizada conforme a la presente Ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

e) Intercambio Electrónico de Datos (EDI). La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto;

f) Sistema de Información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 3. Interpretación. En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4. Modificación mediante acuerdo. Salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III, Parte I, podrán ser modificadas mediante acuerdo.

Artículo 5. Reconocimiento jurídico de los mensajes de datos. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

CAPITULO II Aplicación de los requisitos jurídicos de los mensajes de datos

Artículo 6. Escrito. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

Artículo 7. Firma. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación.

b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

Artículo 8. Original. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

Artículo 9. Integridad de un mensaje de datos. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 10. Admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es

la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

Artículo 11. *Criterio para valorar probatoriamente un mensaje de datos.* Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 12. *Conservación de los mensajes de datos y documentos.* Cuando la Ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta;
2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

Artículo 13. *Conservación de mensajes de datos y archivo de documentos a través de terceros.* El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

CAPÍTULO III Comunicación de los mensajes de datos

Artículo 14. *Formación y validez de los contratos.* En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un

contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Artículo 15. Reconocimiento de los mensajes de datos por las partes. En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

Artículo 16. Atribución de un mensaje de datos.- Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

1. El propio iniciador. 2. Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje, o 3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Artículo 17. Presunción del origen de un mensaje de datos. Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando:

1. Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o

2. El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

Artículo 18. Concordancia del mensaje de datos enviado con el mensaje de datos recibido. Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, éste último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

Artículo 19. Mensajes de datos duplicados. Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el nuevo mensaje de datos era un duplicado.

Artículo 20. Acuse de recibo. Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

a) Toda comunicación del destinatario, automatizada o no, o **b)** Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, y expresamente aquél ha indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recepcionado el acuse de recibo.

Artículo 21. Presunción de recepción de un mensaje de datos. Cuando el iniciador recepcione acuse recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos.

Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que el mensaje de datos recepcionado cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

Artículo 22. Efectos jurídicos. Los artículos 20 y 21 únicamente rigen los efectos relacionados con el acuse de recibo. Las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

Artículo 23. Tiempo del envío de un mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.

Artículo 24. Tiempo de la recepción de un mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará como sigue:

a. Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar:

1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o

2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;

b. Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente.

Artículo 25. Lugar del envío y recepción del mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:

a) Si el iniciador o destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal.

b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

PARTE II COMERCIO ELECTRÓNICO EN MATERIA DE TRANSPORTE DE MERCANCÍAS

Artículo 26. Actos relacionados con los contratos de transporte de mercancías. Sin perjuicio de lo dispuesto en la parte I de la presente ley, este capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea taxativa:

a) **I.** Indicación de las marcas, el número, la cantidad o el peso de las mercancías.

II. Declaración de la naturaleza o valor de las mercancías.

III. Emisión de un recibo por las mercancías.

IV. Confirmación de haberse completado el embarque de las mercancías.

b) **I.** Notificación a alguna persona de las cláusulas y condiciones del contrato.

II. Comunicación de instrucciones al transportador.

c) **I.** Reclamación de la entrega de las mercancías.

II. Autorización para proceder a la entrega de las mercancías.

III. Notificación de la pérdida de las mercancías o de los daños que hayan sufrido;

d) Cualquier otra notificación o declaración relativas al cumplimiento del contrato;

e) Promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;

f) Concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;

g) Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

Artículo 27. Documentos de transporte. Con sujeción a lo dispuesto en el inciso tercero (3º) del presente artículo, en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 26 se lleve a cabo por escrito o mediante documento emitido en papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

El inciso anterior será aplicable, tanto si el requisito en él previsto está expresado en forma de obligación o si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento emitido en papel.

Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío o utilización de un documento emitido en papel, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método confiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

Para los fines del inciso tercero, el nivel de confiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 26, no será válido ningún documento emitido en papel para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos emitidos en papel. Todo documento con soporte en papel que se emita en esas circunstancias deberá contener una declaración en tal sentido. La sustitución de mensajes de datos por documentos emitidos en papel no afectará los derechos ni las obligaciones de las partes.

Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia en un documento emitido en papel, esa norma no dejará de aplicarse a dicho contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en documentos emitidos en papel.

PARTE III FIRMAS DIGITALES, CERTIFICADOS Y ENTIDADES DE CERTIFICACIÓN

CAPÍTULO I Firmas digitales

Artículo 28. Atributos jurídicos de una firma digital. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

- 1) Es única a la persona que la usa.
- 2) Es susceptible de ser verificada.
- 3) Está bajo el control exclusivo de la persona que la usa.
- 4) Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
- 5) Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

CAPÍTULO II Entidades de certificación

Artículo 29. Características y requerimientos de las entidades de certificación. Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones:

- a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación.
- b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley.
- c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

Artículo 30. Actividades de las entidades de certificación. Las entidades de certificación autorizadas por la Superintendencia de Industria y Comercio para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.

2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.

3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la presente Ley.

4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.

5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

6. Ofrecer los servicios de archivo y conservación de mensajes de datos.

Artículo 31. Remuneración por la prestación de servicios. La remuneración por los servicios de las entidades de certificación serán establecidos libremente por éstas.

Artículo 32. Deberes de las entidades de certificación. Las entidades de certificación tendrán, entre otros, los siguientes deberes:

a) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;

b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;

c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;

d) Garantizar la prestación permanente del servicio de entidad de certificación;

e) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;

f) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley;

g) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;

h) Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio;

i) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio;

j) Llevar un registro de los certificados.

Artículo 33. *Terminación unilateral.* Salvo acuerdo entre las partes, la entidad de certificación podrá dar por terminado el acuerdo de vinculación con el suscriptor dando un preaviso no menor de noventa (90) días. Vencido este término, la entidad de certificación revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el suscriptor podrá dar por terminado el acuerdo de vinculación con la entidad de certificación dando un preaviso no inferior a treinta (30) días.

Artículo 34. *Cesación de actividades por parte de las entidades de certificación.* Las entidades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte de la Superintendencia de Industria y Comercio.

CAPÍTULO III Certificados

Artículo 35. *Contenido de los certificados.* Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.
 2. Identificación del suscriptor nombrado en el certificado.
 3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
 4. La clave pública del usuario.
 5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
 6. El número de serie del certificado.
 7. Fecha de emisión y expiración del certificado.
- Artículo 36. *Aceptación de un certificado.*** Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio.

Artículo 37. *Revocación de certificados.* El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos:

1. Por pérdida de la clave privada.
2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

Una entidad de certificación revocará un certificado emitido por las siguientes razones:

1. A petición del suscriptor o un tercero en su nombre y representación.
2. Por muerte del suscriptor.
3. Por liquidación del suscriptor en el caso de las personas jurídicas.
4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso.
5. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.
6. Por el cese de actividades de la entidad de certificación, y
7. Por orden judicial o de entidad administrativa competente.

Artículo 38. *Término de conservación de los registros.* Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular.

CAPÍTULO IV Suscriptores de firmas digitales

Artículo 39. *Deberes de los suscriptores.* Son deberes de los suscriptores:

1. Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.
2. Suministrar la información que requiera la entidad de certificación.
3. Mantener el control de la firma digital.
4. Solicitar oportunamente la revocación de los certificados.

Artículo 40. *Responsabilidad de los suscriptores.* Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.

CAPÍTULO V Superintendencia de Industria y Comercio

Artículo 41. *Funciones de la Superintendencia.* La Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación, y adicionalmente tendrá las siguientes funciones:

1. Autorizar la actividad de las entidades de certificación en el territorio nacional.
2. Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación.
3. Realizar visitas de auditoría a las entidades de certificación.
4. Revocar o suspender la autorización para operar como entidad de certificación.
5. Solicitar la información pertinente para el ejercicio de sus funciones.
6. Imponer sanciones a las entidades de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.
7. Ordenar la revocación de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.
8. Designar los repositorios y entidades de certificación en los eventos previstos en la ley.
9. Emitir certificados en relación con las firmas digitales de las entidades de certificación.
10. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación.
11. Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.

Artículo 42. *Sanciones.* La Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación:

- 1) Amonestación.
- 2) Multas institucionales hasta por el equivalente a dos mil (2.000) salarios mínimos legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades de certificación, hasta por trescientos (300) salarios mínimos legales mensuales vigentes, cuando se les compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.

- 3) Suspender de inmediato todas o algunas de las actividades de la entidad infractora.
- 4) Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.
- 5) Revocar definitivamente la autorización para operar como entidad de certificación.

CAPÍTULO VI Disposiciones varias

Artículo 43. *Certificaciones recíprocas.* Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

Artículo 44. *Incorporación por remisión.* Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a ese mensaje de datos. Entre las partes y conforme a la ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

PARTE IV REGLAMENTACIÓN Y VIGENCIA

Artículo 45. La Superintendencia de Industria y Comercio contará con un término adicional de doce (12) meses, contados a partir de la publicación de la presente ley, para organizar y asignar a una de sus dependencias la función de inspección, control y vigilancia de las actividades realizadas por las entidades de certificación, sin perjuicio de que el Gobierno Nacional cree una unidad especializada dentro de ella para tal efecto.

Artículo 46. *Prevalencia de las leyes de protección al consumidor.* La presente Ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor.

Artículo 47. *Vigencia y Derogatorias.* La presente ley rige desde la fecha de su publicación y deroga las disposiciones que le sean contrarias.”

4. Los mensajes de datos.

4.1. Concepto.

La Ley Modelo de la CNUDMI sobre Comercio Electrónico, define en su artículo 2º, a los mensajes de datos como, la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

Conforme a la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, el concepto de “mensaje de datos” no se limita a la comunicación, sino que pretende también englobar cualquier información consignada sobre un soporte informático que no esté destinada a ser comunicada. En esa tesitura, el concepto de “mensaje” incluye el de información meramente consignada.

Asimismo, se establece que la definición de “mensaje de datos” está formulada en términos por los que se trata de abarcar todo tipo de mensajes generados, archivados o comunicados en alguna forma básicamente distinta del papel.

La definición de “mensaje de datos” pretende abarcar también el supuesto de la revocación o modificación de un mensaje de datos. Se supone que el contenido de un mensaje de datos es invariable, pero ese mensaje puede ser revocado o modificado por otro mensaje de datos.¹²⁷

4.2. Partes

Las partes que interviene en un mensaje de datos son:

a). Por “iniciador” o emisor de un mensaje de datos se entenderá toda persona que, al tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya

¹²⁷ Cfr. León Tovar, Soyla H., González García, Hugo, y Vázquez del Mercado Blanco, Oscar, p.p. 67 y 68.

actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él.

No obstante que en la mayoría de los ordenamientos jurídicos, se utiliza la noción de *parte* o *persona* para designar al titular de derechos y obligaciones, tratándose de mensajes de datos se utiliza el concepto de iniciador.

Los mensajes de datos que se generan automáticamente en una terminal informática o computadora sin intervención humana directa, no significa que se le atribuya a la computadora, la titularidad de derechos y obligaciones, ya que en este caso, cuando se generan en forma automática en una terminal informática sin intervención humana directa, se considera como “iniciados” por la persona propietaria de la terminal.

b) Por “destinatario” de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje de datos, pero que no esté actuando a título de intermediario con respecto a dicho mensaje.

En el marco de la Ley Modelo, por “destinatario” se ha de entender la persona con la cual el iniciador tiene la intención de comunicarse mediante la transmisión del mensaje de datos, por oposición a cualquier persona que pudiera recibir, retransmitir o copiar el mensaje de datos en el curso de la transmisión.

El “iniciador” es la persona que genera el mensaje de datos aun si el mensaje ha sido transmitido por otra persona.

La definición de “destinatario” contrasta con la definición de “iniciador”, que no hace hincapié en la intención. Cabe señalar que, conforme a estas definiciones de “iniciador” y “destinatario”, el iniciador y el destinatario de un determinado mensaje de datos podrían ser una y la misma persona, por ejemplo en el caso en que el autor del mensaje de datos lo hubiera generado con la intención de archivarlo. Sin embargo,

el destinatario que archiva un mensaje transmitido por un iniciador no queda incluido dentro de la definición de “iniciador”.

La definición de “iniciador” debe tenerse por aplicable no sólo al supuesto en el que se genere información para ser comunicada, sino también al supuesto de que se genere información simplemente para ser archivada. Sin embargo, se ha definido “iniciador” en términos destinados a eliminar la posibilidad de que un destinatario de un mensaje de datos que se limita a archivar ese mensaje pueda ser considerado como iniciador del mismo.

c) Por “intermediario”, en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

La Ley Modelo se centra en la relación entre el iniciador y el destinatario, y no trata en general de los derechos y obligaciones de los intermediarios, no obstante, la Ley Modelo no desestima la importancia primordial de los intermediarios en las comunicaciones electrónicas, en virtud de que se necesita la noción de “intermediario” para establecer la necesaria distinción entre iniciadores o destinatarios y terceros.

La definición de “intermediario” pretende abarcar a los intermediarios profesionales y no profesionales, es decir, a cualquier persona, distinta del iniciador y del destinatario, que desempeñe cualquiera de las funciones de un intermediario.

Las principales funciones de un intermediario son: la recepción, transmisión y archivo de mensajes de datos por cuenta de otra persona.

Los operadores de las redes y otros intermediarios pueden prestar servicios adicionales “con valor añadido” como los de formatear, traducir, consignar, autenticar, certificar y archivar los mensajes de datos y prestar además servicios de seguridad respecto de las operaciones electrónicas.

Con arreglo a la Ley Modelo, “intermediario” no se define como categoría genérica sino con respecto a cada mensaje de datos, con lo que se reconoce que la misma persona podría ser el iniciador o el destinatario de un mensaje de datos y ser un intermediario respecto de otro mensaje de datos.¹²⁸

4.3. Identidad del emisor

Conforme a los artículos 90 y 90 bis del Código de Comercio, existe la presunción iuris tantum de que un mensaje de datos ha sido enviado por el emisor o proviene de éste, cuando el mensaje de datos:

- a) Ha sido enviado por el propio emisor.
- b) Ha sido enviado usando medios de identificación del emisor tales como una clave de correo electrónico, una contraseña, la firma electrónica, la FEA, etcétera.
- c) Ha sido enviada por una persona facultada para actuar en nombre del emisor respecto a ese mensaje de datos.
- d) Ha sido enviado por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.
- e) Cuando el destinatario o la parte que confía haya aplicado en forma adecuada el procedimiento acordado antes con el emisor, con el fin de establecer que el mensaje de datos provenía efectivamente de éste, salvo que:
 - i) A partir del momento en que el emisor informe al destinatario o a la parte que confía que el mensaje de datos no provenía de él, y haya dispuesto un plazo razonable para actuar en consecuencia.
 - ii) A partir del momento en que el destinatario o la parte que confía tenga conocimiento, o debiera tenerlo de haber actuado con la debida diligencia o aplicado algún método convenido, de que el mensaje de datos no provenía del emisor.
 - iii) Cuando el mensaje de datos que reciba el destinatario o la

¹²⁸ Cfr. *Ibidem*, p.p. 68-70.

parte que confía resulte de los actos de un intermediario que le haya dado acceso a algún método utilizado por el emisor para identificar un mensaje de datos como propio, con las salvedades de los subincisos 1 y 2 anteriores.

De lo anterior, surge la necesidad de contar con un medio que identifique y asegure que el emisor de mensaje de datos es la persona a quien se atribuye o adjudica, por principio, dicho mensaje.

La ley presume que se actuó con la debida diligencia si el método que uso el destinatario o la parte que confía, cumple con los requisitos para la verificación de la fiabilidad de las firmas electrónicas.

El artículo 1298-A, del citado Código de Comercio, en materia procesal, reconoce de manera expresa como pruebas los mensajes de datos, y previene que para valorar la fuerza probatoria de dichos mensajes se estimará primordialmente la fiabilidad del método en que se generaron, archivaron, comunicaron o conservaron tales mensajes de datos.

Ello supone que si dicho método es perfectamente fiable, entonces quedará demostrado en principio que la información, y por tanto, el acto que de ella emane, proviene del emisor, sin tomar en cuenta si efectivamente el supuesto emisor envió o generó la información.

La ley establece la presunción iuris tantum de que el acto puede ser imputado a una persona determinada, sin embargo, esto nos lleva a considerar que la prueba reconocida por el artículo 1298-A citado, sea tasada con valor probatorio pleno, ya que siempre queda la posibilidad de desvirtuar la presunción legal mediante diversos medios de convicción.

En esa tesitura, la Ley Modelo exige que dicha información sea legible para todos, reproducible, inalterable, susceptible de ser representada ante las autoridades

publicas y autenticable mediante firma.

Antes de la reforma de 2003, cuando el emisor negaba que la información era suya tenía que probarlo por otros medios cuya valoración era difícil, ya que el precepto correspondiente exigía como único medio posible acreditar que la información se había generado en un sistema de información programado por el emisor (aunque la ley no señalaba respecto de esos sistemas programados *para* y no *por* el emisor ni autorizados por éste).

El nuevo precepto señala que el destinatario de la información es quien debe probar la fiabilidad del método que utiliza, que éste cumple con los requisitos previstos para la verificación de la fiabilidad de las firmas electrónicas, es decir, que los datos de creación del mensaje, en el contexto en que se utilizan, corresponden exclusivamente al emisor, que en ese momento estaban bajo su control exclusivo, que es posible detectar cualquier alteración al mensaje de datos hecha después del momento de su envío, y que es posible detectar cualquier alteración del mensaje hecha después de su creación. Tales pruebas o medios de convicción requerirán de la concurrencia de los correspondientes peritos o informes de expertos.

Por su parte el artículo 95, del Código de Comercio, señala que conforme al artículo 90, del mismo ordenamiento, siempre que se entienda que el mensaje de datos proviene del emisor o que el destinatario tenga derecho a actuar con arreglo a este supuesto, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

Finalmente, la ley presume que cada mensaje de datos recibido es un mensaje

de datos diferente, salvo que el destinatario tenga conocimiento, o debiera saber, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que el nuevo mensaje de datos era un duplicado.¹²⁹

4.4. Momento de expedición

Conforme lo dispuesto en el artículo 90 bis, del Código de Comercio, el mensaje de datos se tendrá por expedido y el destinatario o la parte que confía –la que actúa con base en un certificado o una firma electrónica-, en su caso, podrá actuar en consecuencia, cuando:

- a) Haya aplicado en forma adecuada el procedimiento acordado previamente con el emisor, con el fin de establecer que el mensaje de datos provenía efectivamente de éste.
- b) El mensaje de datos que reciba el destinatario o la parte que confía, resulte de los actos de un intermediario que le haya dado acceso a algún método utilizado por el emisor para identificar un mensaje de datos como propio.

Lo anterior, no será aplicable, cuando:

- i) A partir del momento en que el destinatario o la parte que confía, haya sido informado por el emisor de que el mensaje de datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia, o
- ii) A partir del momento en que el destinatario o la parte que confía, tenga conocimiento, o debiera tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, de que el mensaje de datos no provenía del emisor.

La ley presume que se actuó con la debida diligencia si el método que usó el destinatario o la parte que confía cumple con los requisitos establecidos en el Código

¹²⁹ Cfr. *Ibidem*, p.p. 70-72.

de Comercio para la verificación de la fiabilidad de las firmas electrónicas.

Conforme al artículo 91 bis, del Código de Comercio, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo el control del emisor o del intermediario.¹³⁰

4.5. Lugar de expedición y recepción.

Conforme al artículo 94, del Código de Comercio, un mensaje de datos entre el emisor y el destinatario, se entiende por expedido en el lugar donde el emisor tiene su establecimiento y por recibido en el lugar donde el destinatario tiene el suyo. En caso de que el emisor o el destinatario tengan más de un establecimiento, éste será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, el establecimiento principal; si el emisor o el destinatario no tiene establecimiento, se tendrá en cuenta el lugar de su residencia habitual.¹³¹

4.6. Momento de la recepción

Como se ha establecido, en cualquier acto jurídico, determinar el momento en que se da por recibido un mensaje de datos, o en que se tiene conocimiento de su existencia, es de trascendental importancia, debido a la vigencia de las normas que regulan tal acto, e incluso para determinar la capacidad del sujeto que interviene.

Salvo pacto en contrario entre el emisor y el destinatario, el momento de recepción de un mensaje de datos se determinará aun cuando el sistema de información de las partes esté ubicado en un lugar distinto del lugar de su establecimiento, tal como lo expresa el artículo 91, en concordancia con el diverso numeral 94, ambos del Código de Comercio, como sigue:

- a) Si el destinatario ha designado un sistema de información para la

¹³⁰ Cfr. *Ibidem*, p.p. 72 y 73.

¹³¹ Cfr. *Ibidem*, p.p. 73.

recepción de mensajes de datos, éste tendrá lugar en el momento en que ingrese en dicho sistema de información, tenga o no conocimiento el destinatario de la recepción o del contenido del mensaje de datos, aun cuando el sistema de información esté ubicado en un lugar distinto del establecimiento del destinatario.

- b) De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, o de no haber un sistema de información designado, dicho mensaje se tiene por recibido en el momento en que el destinatario recupere el mensaje de datos, aun cuando el sistema de información esté ubicado en un lugar distinto del establecimiento del destinatario.
- c) Si el destinatario no ha designado un sistema de información, la recepción del mensaje de datos tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario, incluso si el sistema de información está ubicado en un lugar distinto del establecimiento del destinatario.
- d) Conforme se entienda que el mensaje de datos proviene del emisor, conforme a lo previsto por el Código de Comercio o que el destinatario tiene derecho a actuar con arreglo a este supuesto, dicho destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador y podrá proceder en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método previamente acordado, que la transmisión daría lugar a un error en el mensaje de datos recibido.

Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo que el destinatario tenga conocimiento, o debiera saber de haber actuado con la debida diligencia, o de haber aplicado algún método previamente

acordado, que el nuevo mensaje de datos era un duplicado.¹³²

4.7. Acuses de recibo

El artículo 14 de la Ley Modelo, establece diversas situaciones:

1). Cuando el iniciador no haya acordado con el destinatario que el acuse de recibo se dé en alguna forma determinada o utilizando un método determinado, se podrá acusar recibo mediante:

- a) Toda comunicación del destinatario, automatizada o no, o
- b) Todo acto del destinatario, que basten para indicar al iniciador que se ha recibido el mensaje de datos.

Esta modalidad es aplicable cuando, al enviar o antes de enviar un mensaje de datos, el iniciador solicite o lo acuerde con el destinatario que se acuse recibo del mensaje de datos.

2). Cuando el iniciador haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo.

3). Cuando el iniciador no haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, si no ha recibido acuse en el plazo fijado o convenido o no se ha fijado o convenido ningún plazo, en un plazo razonable el iniciador:

- a) Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y,

¹³² Cfr. *Ibidem*, p.p.74 y 75.

- b) De no recibirse acuse dentro del plazo fijado conforme al inciso anterior, podrá, dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener.

Esta forma es aplicable cuando, al enviar o antes de enviar un mensaje de datos, el iniciador solicite o lo acuerde con el destinatario que se acuse recibo del mensaje de datos.

4). Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente. Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido.

5). Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

6). Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo, no obedece al propósito de regir las consecuencias jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo.

En ese orden de ideas, el Código de Comercio, en su artículo 92, establece que en lo referente a acuse de recibo de mensajes de datos, se estará a lo siguiente:

- a) Por acuerdo entre las partes, convenido al momento de enviar o antes de enviar el mensaje de datos, o a solicitud del emisor, que se acuse recibo del mensaje de datos, sin que se haya acordado entre éstos una forma o método determinado para efectuarlo. En este supuesto, se podrá acusar recibo del mensaje de datos de manera expresa, ya sea verbal o escrita, mediante cualquier comunicación automatizada o no, o bien de manera tacita mediante cualquier acto del destinatario que baste para indicar al emisor que se ha recibido el mensaje de datos.

- b) Por indicación del emisor que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo. Se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo dentro del plazo fijado por el emisor o dentro de un plazo razonable atendiendo a la naturaleza del negocio, a partir del momento del envío del mensaje de datos.

- c) Por solicitud del emisor o que éste haya acordado con el destinatario que se acuse recibo del mensaje de datos, independientemente de la forma o método determinado para efectuarlo, a menos que el emisor no haya indicado expresamente que los efectos del mensaje de datos estén condicionados a la recepción del acuse de recibo en el plazo solicitado o acordado, o no se haya recibido el acuse de recibo en el plazo solicitado o acordado o, en su defecto, dentro de un plazo razonable atendiendo a la naturaleza del negocio. El emisor podrá dar aviso al destinatario de que no ha recibido el acuse de recibo solicitado o acordado y fijar un nuevo plazo razonable para su recepción, contado a partir del momento de este aviso. Cuando el emisor reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente.

- d) Cuando el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o establecidos en la ley, se presumirá que ello es correcto.¹³³

4.8. Contratos mercantiles celebrados por mensajes de datos

El artículo 11, de la Ley Modelo de la CNUDMI sobre el Comercio Electrónico, establece que en la formación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de

¹³³ Cfr. *Ibidem*, p.p. 75 y 76.

datos. Asimismo, establece que no se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos.

Al respecto, la CNUDMI hace una interpretación sobre dicho numeral, empezando por señalar que la documentación consignada por medios electrónicos, puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, mucha mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos, con tal que se observen ciertos requisitos técnicos y jurídicos; ello, basado en la consideración que se tuvo de ampliar el alcance de conceptos como los de “escrito”, “firma” y “original” con miras a dar entrada al empleo de técnicas basadas en la informática. Criterio que ha sido adoptado por la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional, y la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías.

Derivado de lo anterior, se creó el criterio del equivalente funcional, basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico.

Bajo esa tesitura, la CNUDMI ha interpretado el citado artículo, en su primer numeral, en el sentido de que éste no tiene por objeto interferir con el régimen relativo a la formación de los contratos, sino promover el comercio internacional dando mayor certeza jurídica a la celebración de contratos por medios electrónicos; pues la propia Comisión afirma que, el artículo en mención no trata solamente de la formación del contrato, sino también de la forma en que cabría expresar la oferta y la aceptación de la misma.

Continúa la CNUDMI señalando que, en ciertos países una disposición enunciada en los términos del citado numeral podría considerarse como la mera expresión de algo evidente como que la oferta y la aceptación pueden ser comunicadas por cualquier medio, incluidos los mensajes de datos; no obstante,

aclara la CNUDMI que la disposición es necesaria debido a la incertidumbre que subsiste en numerosos países sobre la posibilidad de que un contrato pueda perfeccionarse válidamente por medios electrónicos; incertidumbre que dimana del hecho de que, en ciertos casos, los mensajes de datos en los que se expresaban la oferta y la aceptación, bien eran generados por una terminal informática sin que hubiera una intervención humana inmediata, dando así lugar a dudas en cuanto a la expresión de voluntad de las partes.

Otra razón de esa incertidumbre, sigue expresando la Comisión, que era inherente a la modalidad de comunicación, debido a la ausencia de un documento escrito; por ello, la propia Comisión consideró necesario el párrafo 1), del citado numeral 11, de la Ley Modelo; en virtud, de que refuerza en el contexto de la formación de un contrato; toda vez que, el hecho de que los mensajes electrónicos puedan tener valor probatorio y surtir algún efecto, no significa necesariamente que puedan ser utilizados para celebrar contratos válidos.

Indica la CNUDMI, asimismo, que el artículo 11 citado, no sólo se debe interpretar en el sentido de que éste prevé conjuntamente la comunicación por vía electrónica, tanto de la oferta como la aceptación, sino también, el caso en que sólo se comunique por esa vía la oferta o la aceptación.

En la Ley Modelo no se pronuncia sobre el lugar y momento de la formación del contrato cuando la oferta o la aceptación de una oferta se expresan por mensaje de datos; ello, expresa la Comisión, se hizo a fin de no interferir con el derecho interno aplicable a la formación del contrato; pues la Comisión consideró que, una disposición de esa índole podría ir más allá del objetivo de la Ley Modelo, que debería limitarse a dar a las comunicaciones electrónicas un grado de certeza jurídica idéntico al de las comunicaciones consignadas sobre papel.

Sin embargo, la Ley Modelo establece en su numeral 15, el tiempo y lugar del envío y la recepción de un mensaje de datos, que en conjunto con el régimen aplicable en el derecho interno a la formación del contrato, tiene como propósito

disipar la incertidumbre sobre el lugar y momento de la formación del contrato cuando la oferta o la aceptación se intercambien electrónicamente.

Sigue interpretando la CNUDMI, que las palabras que “de no convenir las partes otra cosa”, que a la letra dice el artículo 11; se limitan a reiterar el reconocimiento de la autonomía de las partes enunciada en el artículo 4, de la propia Ley Modelo, que tienen por objeto dejar en claro que la finalidad de la Ley Modelo, no es la de imponer el recurso a los medios electrónicos de comunicación a aquellas partes que acostumbren a concertar sus contratos mediante el recurso a la documentación consignada sobre papel.

Por lo que, concluye la CNUDMI, que el artículo 11 no deberá ser interpretado como limitando en modo alguno la autonomía de las partes que no recurran para la negociación de su contrato a formas de comunicación electrónica.

Finalmente, durante la preparación del párrafo 1), del multicitado artículo en comento, la CNUDMI consideró que existía el riesgo de que esta disposición prevaleciera sobre ciertas disposiciones de derecho interno, de lo contrario aplicables, que prescribieran ciertas formalidades para la formación de determinados contratos; entre esas formalidades se incluyen la fe pública notarial y otros requisitos de “escriturización” impuestos por consideraciones de orden público, como la necesidad de proteger a ciertas partes o de advertirlas de ciertos riesgos.

Por esta razón, el párrafo 2), del propio artículo 11, dispone que el Estado promulgante puede excluir la aplicación del párrafo 1) en determinados supuestos que se especificarán en la legislación que promulgue la Ley Modelo.

Por otro lado, el artículo 80 del Código de Comercio, establece que los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.

Asimismo, el artículo 93 del Código de Comercio, establece que cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente. Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de mensaje de datos, siempre que éste sea atribuible a dichas partes.

Así, en los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.¹³⁴

4.9. Valor probatorio a los mensajes de datos.

El artículo 9, de la Ley de la CNUDMI sobre Comercio Electrónico, establece que en todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos: *a)* por la sola razón de que se trate de un mensaje de datos; o *b)* por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.

Asimismo, establece que toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se

¹³⁴ Cfr. *Ibidem*, p.p. 76 y 77.

haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

La CNUDMI, correlaciona este numeral con los artículos 6, 7 y 8, de la propia Ley Modelo, y hace diversos planteamientos al respecto sobre el valor probatorio a los mensajes de datos, asimismo, da un ejemplo la Comisión, en el cual afirma que en algunos ordenamientos jurídicos un documento escrito que no lleve ni fecha ni firma y cuyo autor no se identifique en el escrito o se identifique mediante un simple membrete, sería considerado como “escrito”, pese a su escaso valor probatorio; un documento escrito a lápiz podría ser considerado un “escrito”; un documento fraudulento sería, no obstante, considerado como un “escrito”.

En ese sentido, la CNUDMI afirma que, la finalidad del artículo 6 de la Ley Modelo, que establece que cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta, no es implantar el requisito de que, en todos los casos, los mensajes de datos deben cumplir todas las funciones concebibles de un escrito; sino en fijarse sobre las funciones específicas de éste; por ejemplo, su función probatoria en el contexto del derecho fiscal o su función de advertencia en el contexto del derecho civil.

Por lo tanto, concluye la CNUDMI al respecto, que conviene que las nociones de valor probatorio y de intención de las partes de obligarse, sean tratadas en relación a las cuestiones más generales de la fiabilidad y autenticación de los datos, por lo que no deben incluirse en la definición de escrito.

Esto es, no se debe encuadrar a los mensajes de datos de forma rigorista con el escrito, en cuanto que aquél debe contener todas las funciones del escrito; sino, su equivalencia debe permear en cuanto a las funciones específicas del escrito; bajo la premisa de que la información que contiene el mensaje de datos sea accesible para su ulterior consulta.

El término “accesible”, interpreta la CNUDMI, en el sentido de que se quiere sugerir que la información en forma de datos informatizados debe ser legible e interpretable y que debe conservarse todo programa informático que sea necesario para hacer legible esa información, por lo que no se refiere únicamente al acceso humano, sino también a su procesamiento informático.

En cuanto a la noción de “ulterior consulta”, refiere la CNUMI, que se prefirió a otras nociones como “durabilidad” o “inalterabilidad”, que hubiesen establecido un criterio demasiado estricto, y a nociones como “legibilidad” o “inteligibilidad”, que podrían constituir criterios demasiado subjetivos.

Bajo ese contexto, en las reformas de 29 de mayo de 2000, al artículo 1205, del Código de Comercio, se estableció que son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, *mensajes de datos*, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.

Asimismo, el artículo 1298-A, del citado ordenamiento, adicionado el 29 de mayo de 2000, establece que se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.¹³⁵

4.10. Conservación de mensajes de datos

El artículo 8, de la Ley Modelo, establece que cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que exista alguna garantía fidedigna de que se ha conservado la integridad de la

¹³⁵ Cfr. *Ibidem*, p.p. 77 y 78.

información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma; y, de requerirse que la información sea presentada, dicha información podrá ser mostrada a la persona a la que se deba presentar.

Asimismo, el artículo 10 de la Ley Modelo, establece que cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:

- a) Que la información que contengan sea accesible para su ulterior consulta;
- b) Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y,
- c) Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.

La Ley Modelo refiere que lo anterior no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.

Finalmente, se señala que toda persona podrá recurrir a los servicios de un tercero para observar que ciertos documentos, registros o informaciones sean conservados, siempre que se cumplan con las condiciones indicadas en los incisos a), b) y c), esto es, que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y, que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.

En México, como antecedente se cita que desde 1981, el Código de Comercio en sus artículos 47 y 49, exigía que los comerciantes estuviesen obligados a conservar los originales de todas las cartas, telegramas o documentos en que se consignaran los

contratos, convenios o compromisos que dieran nacimiento a derechos y obligaciones. Ésta conservación debía durar un plazo mínimo de diez años.

Por lo anterior, se adoptaron diversas reformas al Código de Comercio; una de ellas, en su artículo 49, en su párrafo segundo, señala que para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta; en seguida, establece dicho numeral, que la Secretaría de Comercio y Fomento Industrial, hoy Secretaría de Economía, emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

En esa tesitura, la otrora Secretaría de Comercio y Fomento Industrial, emitió la Norma Oficial Mexicana NOM-151-SCFI-2002, publicada en el Diario Oficial de la Federación, el cuatro de junio de 2002, “Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos”.

El objetivo de esta Norma Oficial Mexicana es establecer los requisitos que deben observarse para la conservación del contenido de mensajes de datos que consignen contratos, convenios o compromisos y que en consecuencia originen el surgimiento de derechos y obligaciones; es de observancia general para los comerciantes que deban conservar los mensajes de datos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, así como para todas aquellas personas con quienes los comerciantes otorguen dichos contratos, convenios o compromisos.

Siguiendo este avance sobre la materia, el 29 de agosto de 2003, se adicionó el artículo 93 bis, al Código de Comercio, el cual, establece que sin perjuicio de lo dispuesto en su artículo 49, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un mensaje de datos, en base a los siguientes:

a). Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma.

b). De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

Finalmente, señala que se considerará que el contenido de un mensaje de datos es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.¹³⁶

4.11. El mensaje de datos en el Código de Comercio

El mensaje de datos en los Códigos de Comercio, Civil Federal, Federal de Procedimientos Civiles, Fiscal Federal, y la Ley Federal de Protección al Consumidor, admitieron la existencia legal de los mensajes de datos, con las reformas de 2000 y 2004, basadas en los conceptos de la Ley de la CNUDMI Sobre Comercio Electrónico.

Principalmente, el Código de Comercio, en su artículo 89, parte primera, Libro Segundo (Del Comercio en General), Título Segundo “Del Comercio Electrónico”, establece que las disposiciones de dicho Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte. Asimismo, dicha ley mercantil, enuncia que las actividades reguladas por el Título citado, se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del mensaje de

¹³⁶ Cfr. *Ibidem*, p.p. 79-81.

datos en relación con la información documentada en medios no electrónicos y de la firma electrónica en relación con la firma autógrafa; y, establece que en los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología.

Ello, dilucida la importancia que nuestro legislador dio a efecto de regular los mensajes de datos, no sólo en materia mercantil, sino también civil, administrativa, fiscal, laboral, y demás materias; lo que, representa un avance notable en la materia, y punta de lanza nuestra nación.¹³⁷

Capítulo Segundo

Firma electrónica

Se ha prestado atención a los requisitos de forma que debe contener un documento electrónico, los cuales dotan a éste del grado de fiabilidad, inalterabilidad y rastreabilidad, a saber: escrito, *firma* y original. En esa forma, quedan satisfechos los requisitos jurídicos a los mensajes de datos para que la equivalencia funcional opere.

¹³⁷ Cfr. *Ibidem*, p.p. 82 y 83.

Como definición etimológica de la palabra firma, ésta deriva del verbo “firmar”, y ésta del latín “*firmare*”, cuyo significado es afirmar o dar fuerza.¹³⁸

Según el Diccionario de la Real Academia de la Lengua Española, por “firma” se entiende: “nombre y apellido, o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad o para obligarse a lo que en él se dice.”¹³⁹ Es la “manifestación objetiva”¹⁴⁰ de la persona.

Los tratadistas Planiol y Ripert, la definen de la siguiente forma: “la firma es una inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto”.¹⁴¹

Como antecedentes, se puede mencionar que en Roma, los documentos no eran firmados, ni era costumbre; existía una ceremonia llamada *manufirmatio*, por la cual, luego de la lectura del documento por su autor o el *notarius*, era desplegado sobre una mesa y se le pasaba la mano por el pergamino en signo de su aceptación. Solamente después de cumplir con esta ceremonia se estampaba el nombre del autor, haciéndolo seguidamente los testigos. En el Sistema Jurídico Visigótico, existía la confirmación del documento por los testigos que lo tocaban (*chartam tangere*), signaban o suscribían (*firmatio, roboratio, stipulatio*). En la Edad Media se utilizaron sellos, marcas y signos; Carlo Magno hacía firmar sus actos por un sellero oficial, hasta después comenzó a autenticarse los documentos con sello y firma. Carlos V, en octubre de 1358, obligó en Francia a los escribanos a suscribir los actos que pasaban ante ellos con sus firmas, además de sus signos, y dispuso que los actos del Consejo Real, debían ser autorizados por lo menos tres de los presentes, los que si no supiesen firmar estamparían sus signos. En este tiempo pocas eran las personas que sabían leer y escribir, por lo que generalmente los particulares estampaban en los documentos

¹³⁸ Reyes Krafft, Alfredo Alejandro, *La Firma Electrónica y las Entidades de Certificación*, editorial Porrúa, Sociedad Anónima de Capital Variable, Segunda edición, México 2008, p.p. 85.

¹³⁹ Ídem.

¹⁴⁰ Paganoni O' Donohoe, Francisco Raúl, *Teoría General de los Títulos de Crédito*, O.G.S. Editores, Sociedad Anónima de Capital Variable, Primera edición, México, 2003, pág. 297.

¹⁴¹ Andrés Cápoli, Gabriel, *La Firma Electrónica en el Régimen Comercial Mexicano*, editorial Porrúa Sociedad Anónima de Capital Variable, Primera edición, México, 2004, pág. 3.

que suscribían diversos signos o sellos.¹⁴²

Fue así como la extensión de la instrucción y el desenvolvimiento de las transacciones comerciales, hicieron que la firma fuera adquiriendo relevancia y uso; con el transcurso del tiempo se fue generando como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona; así aparece la firma autógrafa, o sea los trazos o letras o signos que un sujeto estampa con su puño y letra en un documento para asegurar de forma expresa y escrita su voluntad o autoría.

Se ha afirmado que esta evolución se ha acelerado con el fenómeno globalizador, en donde los medios tradicionales se renuevan, y surgen las transacciones y la interacción entre individuos sin vínculos físicos, dando origen a nuevos medios de identificación; surgiendo así, la firma electrónica, cuyo efecto es autenticar un documento digital.

La firma electrónica representa un requisito de forma, necesario para hacer constar por escrito la manifestación de la voluntad de aceptar, contratar o acusar recibo por parte del emisor.¹⁴³

Ha sido adoptada como un mecanismo de seguridad sobre la integridad, origen y autenticidad de un documento electrónico, al amparo de una regulación, e incluso de una certificación.¹⁴⁴ Es un género caracterizado por el soporte, en donde todo modo de identificación de autoría basado en medios electrónicos es firma.¹⁴⁵

De la misma forma que en un documento de papel, la firma electrónica es necesaria como un mecanismo indispensable para proporcionar validez a los actos y contratos que se realizan por medios electrónicos.¹⁴⁶

¹⁴² Cfr. Reyes Krafft, Alfredo Alejandro, ob. cit, pág. 85.

¹⁴³ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 87.

¹⁴⁴ Cfr. Ibidem, p.p. 91.

¹⁴⁵ Cfr. Ibidem, p.p. 93.

¹⁴⁶ Cfr. Ibidem, p.p. 89.

Se busca dar certeza de que las personas que aparecen en tales actos son precisamente quienes se determina que son, por lo que la firma electrónica es el instrumento que otorga seguridad jurídica a tales actos; tal es el caso de los mensajes de datos, los cuales contienen manifestaciones de voluntad que deben atribuirse a una persona determinada para producir consecuencias de derecho y, por tanto, derechos y obligaciones imputables al autor del mensaje.¹⁴⁷

1. Ley Modelo de la CNUDMI sobre las Firmas Electrónicas.

En esa tesitura, dada la importancia que representa reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del empleo de la firma electrónica, la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), aprobó el 5 de julio de 2001, la *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas*.¹⁴⁸

Se ha establecido que esta Ley Modelo tiene por finalidad la de dotar de mayor certeza jurídica al empleo de la firma electrónica, basado en el principio flexible que se enuncia en el artículo 7 de la citada Ley; asimismo, establece la presunción de que toda firma electrónica que cumpla con ciertos criterios de fiabilidad técnica será equiparable a la firma manuscrita.¹⁴⁹

La Ley Modelo adopta un criterio de neutralidad tecnológica para no favorecer el recurso a ningún producto técnico en particular, y define ciertas reglas básicas de conducta que sirven de orientación para evaluar las obligaciones y responsabilidades eventuales de todo firmante, así como de todo tercero que salga de algún modo fiador del procedimiento de firma utilizado y de toda parte en una relación comercial que haya obrado fiándose de la firma.¹⁵⁰

¹⁴⁷ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 90.

¹⁴⁸ www.uncitral.org

¹⁴⁹ Ídem.

¹⁵⁰ Ídem.

A continuación, se reproduce la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas:¹⁵¹

“Ley Modelo de la CNUDMI sobre las Firmas Electrónicas

Artículo 1. Ámbito de aplicación

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No deroga ninguna norma jurídica destinada a la protección del consumidor.

Artículo 2. Definiciones

Para los fines de la presente Ley:

*La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

"La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [...]."

**El término "comercial" deberá ser interpretado en forma lata de manera que abarque las cuestiones que dimanen de toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, aunque no exclusivamente, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; factoraje ("factoring"); arrendamiento con opción de compra ("leasing"); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera.

a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos;

b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;

¹⁵¹ www.uncitral.org

c) Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

d) Por “firmante” se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa;

e) Por “prestador de servicios de certificación” se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas;

f) Por “parte que confía” se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Artículo 3. Igualdad de tratamiento de las tecnologías para la firma

Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1 del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

Artículo 4. Interpretación

1. En la interpretación de la presente Ley se tendrán en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y de asegurar la observancia de la buena fe.

2. Las cuestiones relativas a las materias que se rigen por la presente Ley que no estén expresamente resueltas en ella se dirimirán de conformidad con los principios generales en los que se basa esta Ley.

Artículo 5. Modificación mediante acuerdo

Las partes podrán establecer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 6. Cumplimiento del requisito de firma

1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y

resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.

2. El párrafo 1 será aplicable tanto si el requisito a que se refiere está expresado en forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3. La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1 si:

a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

4. Lo dispuesto en el párrafo 3 se entenderá sin perjuicio de la posibilidad de que cualquier persona:

a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1, la fiabilidad de una firma electrónica; o

b) aduzca pruebas de que una firma electrónica no es fiable.

5. Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 7. Cumplimiento de lo dispuesto en el artículo 6

1. *[La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia]* podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6 de la presente Ley.

2. La determinación que se haga con arreglo al párrafo 1 deberá ser compatible con las normas o criterios internacionales reconocidos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 8. Proceder del firmante

1. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme al artículo 9 de la presente Ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:

- i)* el firmante sabe que los datos de creación de la firma han quedado en entredicho; o
- ii)* las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.

2. Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1.

Artículo 9. Proceder del prestador de servicios de certificación

1. Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales;

c) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:

- i)* la identidad del prestador de servicios de certificación;
- ii)* que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

- iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

- i) el método utilizado para comprobar la identidad del firmante;
- ii) cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;
- iii) si los datos de creación de la firma son válidos y no están en entredicho;
- iv) cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;
- v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado *b)* del párrafo 1 del artículo 8 de la presente Ley;
- vi) si se ofrece un servicio para revocar oportunamente el certificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado *d)*, proporcionar un medio para que el firmante dé aviso conforme al apartado *b)* del párrafo 1 del artículo 8 de la presente Ley y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado *d)*, cerciorarse de que existe un servicio para revocar oportunamente el certificado;

f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.

2. Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1.

Artículo 10. Fiabilidad

A los efectos del apartado *f)* del párrafo 1 del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

- a)* los recursos humanos y financieros, incluida la existencia de activos;
- b)* la calidad de los sistemas de equipo y programas informáticos;

c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;

e) la periodicidad y el alcance de la auditoría realizada por un órgano independiente;

f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; o

g) cualesquiera otros factores pertinentes.

Artículo 11. Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

a) verificar la fiabilidad de la firma electrónica; o

b) cuando la firma electrónica esté refrendada por un certificado:

i) verificar la validez, suspensión o revocación del certificado; y

ii) tener en cuenta cualquier limitación en relación con el certificado.

Artículo 12. Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras

1. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:

a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni

b) el lugar en que se encuentre el establecimiento del expedidor o del firmante.

2. Todo certificado expedido fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que todo certificado expedido en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.

3. Toda firma electrónica creada o utilizada fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que toda firma electrónica creada o utilizada en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.

4. A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines del párrafo 2, o del párrafo 3, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5. Cuando, sin perjuicio de lo dispuesto en los párrafos 2, 3 y 4, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.”

Cabo Verde (2003), China (2004), Guatemala (2008), Jamaica (2006), los Emiratos Árabes Unidos (2006), México (2003), Tailandia (2001) y Viet Nam (2005), han promulgado legislación basada en la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas. Asimismo, Costa Rica (2005) y la India (2009). han promulgado legislación influenciada por los principios que la Ley Modelo fue embasada, en donde el año de promulgación que se indica corresponde al año en que el órgano legislativo competente adoptó la legislación, no así indica el año de la entrada en vigor de la legislación de que se trate.¹⁵²

2. Tipos de firma electrónica.

La Ley Modelo sobre las Firmas Electrónicas, da un concepto general de firma electrónica, al establece que por firma electrónica se entenderá los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

En México, el oficio circular por el que se emiten los Lineamientos para la Operación de los Sistemas Electrónicos de la Subsecretaría de Egresos, define la firma electrónica como, “la cadena de caracteres procesados y protegidos a través de

¹⁵² www.uncitral.org

sistemas electrónicos que identifican, autentican y proveen de certeza a los trámites presupuestarios realizados por el usuario, equiparable a la firma autógrafa. Es un conjunto de datos que adjunta y asocia, en forma lógica, a un documento electrónico con un usuario, de forma tal que constituye un medio de identificación electrónica.”¹⁵³

Ahora bien, de acuerdo a la clasificación que hace el Código de Comercio, en su artículo 89, se puede clasificar la firma electrónica en los siguientes: i) *firma electrónica* o *firma electrónica simple*; ii) *firma electrónica avanzada* o *fiabile*; y, iii) *firma digital*.

2.1. Firma electrónica simple (FE)

El Código de Comercio, establece en su artículo 89, que la firma electrónica (simple), son los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Se ha considerado que la firma electrónica simple es el término genérico y neutral que se utiliza para referirse al universo de tecnologías mediante las cuales una persona puede identificar como suyo (firma) un mensaje de datos.

Es decir, la firma electrónica simple, es el conjunto o bloque de caracteres, datos, códigos o claves criptográficas privadas, en forma electrónica, que se adjuntan, asocian o anexan a un mensaje de datos, para designar al autor del mismo; que no implica necesariamente que el mensaje esté encriptado, esto es, que no pueda ser leído por otras personas.¹⁵⁴

¹⁵³ León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 92.

¹⁵⁴ Cfr. Ibidem, p.p. 95.

Firmar un mensaje de datos con una FE, es similar a firmar un documento holográficamente, en donde éste puede ser visto por otras personas.¹⁵⁵

Como ejemplos de firma electrónica simple se encuentran:¹⁵⁶

- El nombre del emisor al final de un correo electrónico.
- La digitalización de una firma como archivo gráfico.
- Un número de identificación personal (NIP).
- Ciertas biometrías utilizadas para efectos de identificación (huella digital o retina).
- La firma que aparece en la credencial para votar, licencia de manejo, pasaporte, etcétera.

Desde 1999 en México, se empezó a estudiar lo relativo a las firmas electrónicas, y el diecisiete de enero de dos mil dos, se emitió un acuerdo publicado en el Diario Oficial de la Federación, en el cual se permite el uso de medios electrónicos para la simplificación, aunque sólo considera su utilización en las promociones que los particulares formulan en los procedimientos administrativos.¹⁵⁷

La FE es la firma electrónica que se ha utilizado hasta ahora para remitir las declaraciones a la autoridad fiscal por Internet, a través de la página del Sistema de Administración Tributaria (SAT). Además, se requiere el empleo de la FE para acceder a aplicaciones sobre consulta de transacciones y reimpresión de acuses, en el esquema de pagos electrónicos.¹⁵⁸

La firma electrónica simple encuentra su fundamento en los artículos 97 del Código de Comercio, y 17-D, primer párrafo, del Código Fiscal de la Federación.

¹⁵⁵ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 95.

¹⁵⁶ Ídem.

¹⁵⁷ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 96.

¹⁵⁸ Ídem.

El artículo 97 del Código de Comercio, establece que cuando la ley requiera o las partes acuerden la existencia de una firma en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si se utiliza una firma electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese mensaje de datos.

Asimismo, el artículo 17-D, del Código Fiscal de la Federación, no obstante establece que cuando las disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor, asimismo, señala que las autoridades fiscales, mediante reglas de carácter general, podrán autorizar el uso de otras firmas electrónicas.

En observancia a la información contenida que se ha realizado en la pagina web del SAT, más de dos millones de contribuyentes cuentan con su firma electrónica, conocida también como clave de identificación electrónica confidencial (CIEC), la cual es un sistema de identificación basado en el RFC y el NIP, que se utiliza para realizar las declaraciones provisionales y las declaraciones anuales.

2.2. Firma digital

Considerada por el legislador en el Código de Comercio, como una *especie* de la firma electrónica.

Es un bloque de caracteres que acompaña a un documento o archivo, y acredita quién es el autor (autenticación) del mismo, y que no ha existido ninguna manipulación posterior de los datos (integridad). Se trata de cierto tipo de firma electrónica basada en el uso de criptografía; la más comúnmente utilizada es la llamada criptografía asimétrica o de llave pública.¹⁵⁹

¹⁵⁹ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 98.

Puede ser definida como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación de un algoritmo (fórmula matemática) de cifrado asimétrico o de llave pública, a un mensaje determinado. Este algoritmo equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje. Asimismo, esta firma permite determinar de forma fiable que el emisor del mensaje de datos es realmente la persona que dice ser, así como si el contenido del documento ha sido alterado o no posteriormente; esto es, permite asegurar la identidad del firmante y la integridad del mensaje.¹⁶⁰

Desde el punto de vista tecnológico, la firma digital es una cadena o secuencia de caracteres que se adjunta o asocia al final del cuerpo de un mensaje. La firma digital se crea mediante el uso de la *criptografía de llave pública*.¹⁶¹

En este tipo de criptografía se utiliza una llave privada para firmar un mensaje y una pública para leerlo; el mensaje se encripta con la llave privada, de tal forma que cualquiera puede desencriptarlo utilizando la llave pública. El dueño de la llave privada es el único que puede encriptar el documento (mensaje de datos), por lo que la firma digital garantiza que es él quien envió el documento. Para firmar un documento digital, el emisor utiliza su propia llave privada, a la que sólo él tiene acceso. De esta manera, el autor queda vinculado al documento que firma. En este caso, cualquier persona puede verificar la validez de una firma si dispone de la llave pública correspondiente.¹⁶²

2.3. Firma electrónica avanzada (FEA/FIEL)

El Código de Comercio pone el adjetivo de *fiable* a esta firma, y considera en este tipo a la firma electrónica que cumpla con los siguientes requisitos: *i*). Que los datos de creación de la firma, en el contexto en que son utilizados, correspondan exclusivamente al firmante; *ii*). Que en el momento de la firma, estén bajo el control

¹⁶⁰ Ídem.

¹⁶¹ Ídem.

¹⁶² Ídem.

exclusivo del firmante, los datos de creación de la firma; *iii*). Que se posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; *iv*) Respecto a la integridad de la información de un mensaje de datos, sea posible detectar cualquier alteración de ésta hecha después del momento de la firma. No obstante lo anterior, el propio código mercantil citado, deja la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una firma electrónica, o presente pruebas de que una firma electrónica no es fiable.

Por su parte, el Código Fiscal de la Federación, no define la FIEL, sin embargo, en el artículo 17 D, establece que cuando las disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos que establezcan una regla diferente; para tal efecto, se deberá contar con un certificado que confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, expedido por el Servicio de Administración Tributaria cuando se trate de personas morales, y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas.

De lo que se desprende, que en un documento digital una firma electrónica avanzada amparada por un certificado vigente produce los efectos siguientes:

- a. Sustituye a la firma autógrafa del firmante.
- b. Garantiza la integridad del documento.
- c. Produce los mismos efectos que las leyes otorgan a los documentos con firma autógrafa y tiene el mismo valor probatorio.

Asimismo, cabe destacar la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios, publicada en la Segunda Parte del Periódico Oficial del Estado de Guanajuato, el 9 de julio de 2004; la cual en su artículo 2º, denomina este tipo de firma electrónica avanzada, como *firma electrónica certificada*, y la define como aquella que ha sido certificada por la autoridad certificadora en los términos que señale esta Ley, consistente en el conjunto

de datos electrónicos integrados o asociados inequívocamente a un mensaje de datos que permite asegurar la integridad y autenticidad de ésta y la identidad del firmante.

3. Firma electrónica avanzada (FEA/FIEL)

3.1. Concepto.

Como ya se ha dicho con antelación, la firma electrónica avanzada es un conjunto o bloque de caracteres, códigos o claves criptográficas privadas en forma electrónica, que viaja junto, asociado o anexo a un documento digital, y mediante el cual se acredita quién es el autor o emisor del mismo.¹⁶³

Es una cadena de caracteres procesados protegidos a través de sistemas electrónicos que identifican, autentican y proveen certeza a los actos realizados por el emisor. La FIEL es equiparable a la firma autógrafa, y constituye un medio de identificación electrónica, que necesariamente debe contar con: i). un certificado digital; ii). una clave de acceso, y iii). una contraseña, la cual autoriza a un tercero denominado unidad certificadora o prestador de servicios de certificación (PSC), previa solicitud.¹⁶⁴

3.2. Confiabilidad de la firma electrónica avanzada.

La firma electrónica es fiable, en virtud de que ésta debe contener los siguientes requisitos, mismos que establece el artículo 6º, de la Ley Modelo, recogidos en el Código de Comercio, en el artículo 97, a saber:

1. Que los datos de creación de la firma, en el contexto en que son utilizados, correspondan exclusivamente al firmante.
2. Que los datos de creación de la firma estén, en el momento de la firma, bajo el control exclusivo del firmante.

¹⁶³ León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 99.

¹⁶⁴ Ídem.

3. Que sea posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma.
4. Que sea posible detectar cualquier alteración de la información de un mensaje de datos, después del momento de la firma, para dar seguridad en cuanto a la integridad de la información.

Asimismo, en la parte final del segundo numeral citado, se establece que la firma electrónica, se considerará como fiable sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una firma electrónica; o presente pruebas de que una firma electrónica no es fiable.

Según, lo dispuesto en el artículo 7 de la Ley Modelo, recogido por el Código de Comercio, en el artículo 98; una institución (certificadora de firmas), podrá determinar qué firmas electrónicas son fiables, conforme a las normas o criterios internacionales reconocidos, y sin perjuicio de la aplicación de las normas de derecho privado.

3.3. Certificación.

Para dar fiabilidad a la firma, se exige la presencia de un tercero, una persona física o moral, de derecho público o privado, que preste servicios de certificación para auxiliar y determinar que las firmas electrónicas son fiables; estos son llamados prestadores de servicios de certificación (PSC).

Los prestadores de servicios de certificación, determinarán y harán del conocimiento de los usuarios si las firmas electrónicas avanzadas o fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 97, previamente citado, referente a los requisitos que integra la firma electrónica avanzada.

El PSC siempre deberá utilizar, al prestar sus servicios, sistemas, procedimientos, y recursos humanos fiables, y la determinación que haga deberá ser compatible con las normas o criterios internacionales reconocidos, sin perjuicio de la aplicación de las normas de derecho internacional privado.

La FIEL amparada por un documento (certificado) emitido por el PSC, permite la identificación del signatario, ya que se crea por medios que el signatario mantiene bajo su exclusivo control.

La FIEL, proporciona conforme a los procedimientos y métodos de creación de la misma, lo siguiente:

- a) Autenticación. Asegura que una persona determinada sea la indicada para llevar a cabo una operación concreta e identifica al emisor del mensaje de datos. También permite identificar a la persona que realiza el acto, esto es, verifica la autoridad del firmante para asegurar que fue él y no otro el autor del documento.
- b) Confidencialidad. Garantiza que nadie más vea los intercambios de datos que se lleven a cabo, toda vez que la información está cifrada. La información cifrada no puede descifrarse si no se tiene la llave privada.
- c) Integridad. Asegura que la información no se modifica o altera de manera fortuita o deliberada durante el trayecto o el almacenaje de la misma, y que no puede ser modificada por un tercero antes, durante o después de la firma.
- d) No repudiación. Garantiza que el emisor fue quien firmó el documento. Seguridad de que el autor del documento no se retracte en un futuro de las opiniones o acciones asignadas en el mensaje de datos. A partir de la recepción de los medios de identificación electrónica, el titular acepta las consecuencias y alcance probatorio del uso de los mismos y de los documentos que se generen.¹⁶⁵

La cualidad de que la firma sea generada por el usuario mediante medios que mantiene bajo su propio control (clave privada protegida, contraseña, datos

¹⁶⁵ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 104.

biométricos, tarjeta chip, etc.), asegura la imposibilidad de llevar a cabo lo que se conoce como suplantación de personalidad.¹⁶⁶

3.4. Cómo se firma un documento digital.

En los documentos físicos o tangibles, el autor utiliza tinta para firmarlos de su puño y letra, produciendo signos o trazos de su puño y letra. En un documento digital, se puede firmar de distintas formas; por ejemplo, cuando se teclea el nombre del emisor en un mensaje de correo electrónico, cuando se digitaliza o “escanea” la firma del emisor y se reproduce en el documento digital, cuando se inserta un “NIP” o la CIEC, al hacer clic en el botón “Acepto” u “OK”, o cuando se utiliza la FIEL.¹⁶⁷

Cuando un usuario quiere firmar un documento y lo genera mediante algún programa (Word, Excel o Power Point), se crea un proceso llamado *digestión* del documento. En este proceso, un algoritmo Hash genera huellas digitales que permiten validar la integridad del mensaje y ayudan a detectar que no haya modificación alguna. El resultado de esa digestión se cifra con una llave privada, conformando la firma digital. Cada vez que se firma un documento, el resultado de la firma se obtiene de manera diferente, lo que constituye un elemento de seguridad. Al finalizar el proceso, la firma se asocia lógicamente con el documento y éste se envía al destinatario, quien recibe el mensaje y la huella digital. Para que el destinatario identifique tanto al emisor como al documento firmado, primero se genera un proceso de digestión del documento puro de modo que se obtenga un resultado de 16 a 20 bits (la huella del documento); luego, se descifra la firma digital que se envió con la llave pública del emisor y se comparan las huellas digitales para validar la integridad de la información. Si coinciden, el documento se considera íntegro.¹⁶⁸

El destinatario verificará asimismo lo siguiente: que el certificado digital sea emitido por un PSC; que el certificado digital no haya expirado; que el certificado no

¹⁶⁶ Cfr. *Ibidem*, p.p. 105.

¹⁶⁷ *Ídem*.

¹⁶⁸ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 106.

esté revocado, para lo cual deberá revisarlas listas de revocación o preguntar al PSC; si es posible descifrar la firma electrónica utilizando la llave pública (de ser así, el documento es auténtico); finalmente, si la información recibida, al compararla con la documentación derivada de la digestión, la huella digital es la misma, el documento es íntegro.¹⁶⁹

3.5. Diferencias entre firma electrónica y FEA(FIEL).

La diferenciación que tienen los documentos amparados por la firma electrónica (simple) y la firma electrónica avanzada, radica en la protección legal.

La firma electrónica simple autentica la identidad del autor de un mensaje de datos y muestra la cédula de identidad par confirmar la autoría; pero no asegura la identidad ni la integridad del mensaje, ni de la firma.

La firma electrónica avanzada, también autentica la identidad del autor de un mensaje de datos; con la diferencia de que ésta permite asegurar que la persona a quien se le atribuye es precisamente quien dice ser; por lo que, los efectos jurídicos que produce la FIEL son consecuencia de que representa la voluntad de la persona que ha participado en la celebración del acto en cuestión.

En ese sentido, la FIEL permite la identificación del signatario, y ha sido creada por medios que éste mantiene bajo su estricto control, de tal forma que está vinculada únicamente al mismo y a los datos a los que se refiere.

Por lo que, la firma electrónica avanzada garantiza la autenticación de las partes, la integridad del documento y que los firmantes no podrán repudiar dicho mensaje; esto es, no podrán negar su existencia y validez.

Se destaca que el uso de esta firma permite que sea detectable cualquier modificación ulterior de los datos contenidos en el mensaje que ampara, por lo que, el

¹⁶⁹ Ídem.

objetivo de la FIEL es garantizar que la información que viaja, como lo es a través de Internet, el correo electrónico, EDI o fax, asociado al mensaje de datos; circule de manera segura y confidencial.¹⁷⁰

3.6. La firma electrónica avanzada como requisito del elemento formal en los actos jurídicos.

Como se ha visto con antelación, la firma electrónica es aquella consignada en un mensaje de datos o documento electrónico. Este documento electrónico puede revestir la figura de un contrato electrónico. Como sucede con el contrato escrito, requiere para su existencia del consentimiento y el objeto. De la misma forma, el contrato electrónico requiere para su existencia de dichos elementos.

El consentimiento en los contratos electrónicos es expreso, en virtud, de que la voluntad tratándose de la naturaleza de estos documentos, se manifiesta por medios electrónicos, según lo dispone el artículo 1803, fracción I, del Código Civil Federal.

“Artículo 1803. El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente: - - - I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.”.(resalto)

Lo anterior, se robustece con lo establecido por los artículos 1834 y 1834 bis, del citado código sustantivo, los cuales señalan respectivamente, que cuando se exija la forma escrita para el contrato, los documentos relativos deben ser firmados por todas las personas a las cuales se imponga esa obligación; teniéndose por cumplido dichos supuestos, cuando se utilicen medios electrónicos, ópticos o de cualquier otra tecnología; siempre que la información generada o comunicada en forma íntegra, a

¹⁷⁰ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, págs. 106 y 107.

través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta.

En esa tesitura, la Guía Jurídica de comercio electrónico, da las siguientes características de la firma electrónica avanzada:

- a) Dotar a las partes de la prueba de la existencia y naturaleza de la intención de las partes.
- b) Determinar el nacimiento de derechos y obligaciones para las partes.
- c) Advertir a las partes de los alcances y las consecuencias de celebrar un contrato o realizar un acto.
- d) Facilitar su reproducción para que cada una de las partes pueda disponer de un ejemplar y facilitar las tareas de control o de verificación ulterior para fines contables, fiscales o reglamentarios.
- e) Proporcionar un documento presentable ante las autoridades y tribunales.
- f) Dar expresión definitiva de la intención del autor y dejar constancia de ella.
- g) Proporcionar un soporte material que facilite la conservación de los datos en forma visible.
- h) Proporcionar un documento que sea legible para todos, inalterable (que permita dejar constancia permanente de la operación) y accesible para ulterior consulta.¹⁷¹

Así, tenemos que las funciones de la FIEL son:

1. Identificar al emisor del mensaje de datos.
2. Dar certeza a la participación personal de esa persona en el acto de firmar.
3. Asociar a esa persona con el contenido de un documento.

¹⁷¹ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 109.

4. Demostrar la intención de una parte contractual de obligarse por el contenido del contrato firmado.
5. Demostrar la intención de una persona de reivindicar la autoría de un texto.
6. Demostrar la intención de una persona de asociarse con el contenido de un documento escrito por otra, y el hecho de que esa persona había estado en un lugar determinado, en un momento dado.¹⁷²

3.7. Elementos que participan en la FEA(FIEL)

Para efecto de comprender la implementación de la firma electrónica avanzada es necesario describir los siguientes elementos:¹⁷³

1. **Información.** Es todo conjunto de datos representados de forma escrita, gráfica, auditiva o visual, que ofrece un conocimiento o pensamiento. El autor Claude Shannon, precursor de la *teoría de la información*, quien dándose cuenta de las cualidades poco atractivas de la palabra información, en 1948, tituló su artículo “Una teoría matemática de la comunicación”, en la que pronuncia que cuanto mayor y mejor sea la información, menor será el desconocimiento en las personas. En esta publicación quedó demostrado que la información (la voz de las personas, las conversaciones telefónicas, las emisiones de radio y la televisión, la telegrafía, las publicaciones escritas, etcétera), puede ser medida y cuantificada.

Este autor describe con precisión el proceso de la comunicación y su susceptibilidad de ser operado a través de un sistema eléctrico digital, y establece las bases para cuantificar toda clase de información, donde plantea que cualquier dato (base de información) puede ser expresado en unos (1) y ceros (0) y, por tanto, puede ser transmitido a través de circuitos eléctricos.

Estos circuitos se basaron originalmente en relevadores, después se utilizaron los bulbos, y actualmente, se usan millones de transistores interconectados entre sí

¹⁷² Ibidem, p.p. 110.

¹⁷³ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit. p.p. 211-222.

dentro de chips de muy pequeñas dimensiones y de muy bajo consumo de energía.

La teoría de la información se enfoca en la solución de los problemas técnicos de las telecomunicaciones, no así en la explicación del fenómeno de la comunicación interpersonal como una experiencia social.

Actualmente, la teoría de la información establece que la información puede tratarse como una cantidad física medible en *bits*, de tal manera que puede transmitirse, almacenarse, procesarse y expresarse.

El bit, se considera la unidad básica de medición de la información. A la electrónica capaz de procesar la información en forma de bits, se le conoce como *electrónica digital*. Para hacer referencia a la cantidad de información digital es más común utilizar el término *bite*. Un byte es un conjunto de 8 bits. Cuando la información es cuantiosa, se utilizan otras unidades de medición, el megabyte (MB), que equivale a un millón de bytes y el gigabyte, que equivale a mil millones de bytes.

2. Digitalización. Cuando la información se digitaliza, se somete a un proceso de conversión de su representación tradicional a un formato binario (bits), utilizando ciertos patrones o reglas que toman diversas muestras lo suficientemente significativas para reconstruir posteriormente la información sin perder el mensaje original. La información en forma de bits, se puede expresar a través de los siguientes:

- a. Texto. Es aquella información expresada en forma de caracteres alfanuméricos y una serie de signos de puntuación que pertenecen a cierto alfabeto conocido.
- b. Gráfico. Es aquella información expresada en forma de imagen estática de un solo color o multicolor.
- c. Audio. Es aquella información en forma de sonido perceptible al oído humano.
- d. Video. Es aquella información en forma de secuencias de múltiples imágenes perceptibles por la vista que transmiten la sensación del movimiento.

3. **Encriptación.** Es un proceso mediante, el cual, la información se convierte en algo completamente indescifrable para cualquier persona que no sea el destinatario o el propietario. Es una técnica que permite proteger la información al transformar los datos en algo totalmente incompresible y reconstruirlos después cuando así se requiera.

Para realizar el proceso de encriptación es necesario además del mensaje o documento a encriptar, un valor independiente llamado *llave de encriptación*. Cuando se desencripta necesitamos otro valor, que en este caso de le llama *llave de desencriptación*. Este proceso es en realidad una operación matemática sobre un número entero utilizando números primos. Es necesario recordar que los números primos son aquellos divisibles sólo por sí mismos y por la unidad; por ejemplo, 2,3,5,7,11,13,17,19,23,29,31. Por definición se trata de números naturales por lo que únicamente pueden ser números enteros positivos y son infinitos. Segundo, la operación matemática llamada módulo (*mod*) se define como el número entero (sin decimales) que resulta de la división entre dos números, es decir:

$$\mathbf{a \text{ mod } b = \text{entero (sin decimales) resultante de } \mathbf{a/b}}$$

En términos generales el método de encriptación utilizado en la firma electrónica avanzada se centra en la obtención de dos números primos (p,q) del mismo tamaño, que multiplicados entre sí dan por resultado un número entero (n). En conjunto (p,q) se conoce como llave privada y (n) como llave pública, y se utilizan siempre números enteros bastante grandes, tales como números de 308 dígitos expresados en 1024 bits.

En la práctica existen dos tipos de encriptación: *simétrica* y *asimétrica*.

La encriptación simétrica sucede cuando la llave de encriptación y la llave de desencriptación son idénticas.

La encriptación asimétrica ocurre cuando la llave de encriptación, es diferente a la llave de desencriptación. En este caso dichas llaves son llamadas pública y privada. A este método se le conoce como PKI (*Public Key Infrastructure*).

El método asimétrico es el indicado para la implementación de la firma electrónica.

Existen dos maneras de utilizar este método. En la primera, para garantizar al destinatario que el emisor es quien dice ser, el emisor encripta el mensaje con su llave privada y el destinatario lo desencripta con la llave pública del emisor. En la segunda, para garantizar al emisor que sólo el destinatario autorizado podrá leer la información, el emisor encripta con la llave pública del destinatario y el destinatario desencripta con su llave privada.

En ambos casos la llave privada de los dos interlocutores deberá permanecer protegida bajo la responsabilidad del propietario de la llave. Es común la utilización de ambas formas de manera conjunta, aplicando primero la encriptación con la llave privada del emisor y enseguida encriptando con la llave pública del destinatario, lo que garantiza que el emisor es quien dice ser y que sólo el destinatario autorizado podrá leer la información. Esta doble encriptación es un método de protección de la información eficaz.

En México, el llamado RSA (Rivest, Shamir y Adleman), es el estándar que define el procedimiento para implementar la encriptación, adoptado por el SAT para la implementación de la firma electrónica avanzada.

El algoritmo asimétrico tiene el inconveniente de ser lento, por lo que, no es útil para aplicarlo en todos los casos para cifrar mensajes digitales, en especial si son éstos de gran tamaño; toda vez que, entre más grande sea el mensaje más lento es el proceso de encriptación asimétrico. Por ello, se ha utilizado una función matemática que produce un resumen o compendio de tamaño pequeño y fijo, sin importar el tamaño del mensaje original; posteriormente, se aplica la encriptación a dicho resumen.

Esta función garantiza que no se encuentren dos mensajes diferentes que generen un resumen idéntico, aun cuando la diferencia de ambos sea de sólo un signo de puntuación. A este proceso matemático de obtener un resumen único de tamaño fijo y pequeño, se le llama *función Hash*.

Se ha destacado que las funciones básicas de la encriptación son: la *autenticación*, *confidencialidad* y la *integridad*.

La autenticación, en cuanto a que permite al destinatario asegurarse de que el emisor es quien dice ser, y permite al emisor tener la certeza de que sólo el destinatario recibirá el mensaje. La confidencialidad refiere a que la encriptación garantiza que ninguna persona ajena tenga acceso al contenido del mensaje durante su transmisión o almacenaje. Y, la integridad de esta técnica refiere a que garantiza que el mensaje estará intacto.

3.8. Requisitos de seguridad de la FEA(FIEL)

Fundamentalmente, la firma electrónica avanzada cumple con los siguientes requisitos:

1. Integridad. Garantiza que el documento firmado está completo y no ha sufrido la mas mínima alteración.
2. Autenticidad. Garantiza que el autor del documento es quien dice ser y que está plenamente identificado. Esta característica garantiza la integridad, por lo que si un documento es auténtico también es íntegro, pero no en sentido contrario.
3. No repudio. Garantiza que el autor del documento no puede rechazar su autoría con el argumento que no se trata del documento que éste ha firmado. Es requisito es condición suficiente para la autenticidad, por lo que si un documento es no repudiable se considera auténtico y por tanto íntegro, pero no a la inversa.
4. Confidencialidad. Garantiza que sólo las personas autorizadas

pueden obtener el contenido del documento en texto claro.¹⁷⁴

3.9. Proceso para implementar la FEA(FIEL).

El proceso que se distingue para implementar la firma electrónica avanzada, es a saber:

1. Generación de llaves (pública y privada). A través de un software se generan números primos de gran tamaño en forma pseudoaleatoria para procesarlos matemáticamente con un conjunto de datos básicos confidenciales de identificación personal ya digitalizados, tales como el nombre completo, el correo electrónico, un par de contraseñas, etcétera. Estos datos se consideran los datos de creación de la FEA. Con este software se obtiene un par de llaves (pública= n,e y privada = p,q). La llave privada se conserva en un archivo tipo *.key. Para poder utilizar posteriormente dichas llaves se requiere conocer las contraseñas que el propietario estableció en forma confidencial en dicho software, una contraseña para acceder al proceso de firma y la otra para solicitar la revocación del certificado digital actual. Para aplicaciones en las que se requiere de un nivel más alto de seguridad se suele recurrir a tarjetas electrónicas inteligentes como SmartCard, PCMCIA; donde se almacene la llave privada. Estas tarjetas sólo pueden utilizarse si se conoce un número personal secreto llamado *NIP*, el cual, garantiza que la tarjeta no se podrá utilizar por un tercero que desconozca el NIP.
2. Requerimiento de certificado digital. Generalmente, se genera un requerimiento de certificado digital mediante el mismo software que se utilizó para generar las llaves pública y privada. Este requerimiento se encripta con la llave privada del firmante de tal manera que se produce otro archivo del tipo *.req. El requerimiento

¹⁷⁴ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 225.

se entrega a una entidad certificadora autorizada, junto con una serie de documentos legales que acreditan la identidad, por lo general en una cita a la que se asiste personalmente.

3. Generación de certificado digital. Se utiliza el archivo de requerimiento (*.req) y asociándolo con la información probatoria de la identidad del firmante, una entidad certificadora autorizada genera un certificado digital mediante software especial. En la práctica el certificado es un archivo que se utilizará en el proceso de firma electrónica. Este archivo es del tipo *.cer.¹⁷⁵

Para que una firma electrónica se considere FIEL debe contar con los siguientes elementos:

1. Emisor y destinatario plenamente identificados ante un prestador de servicios de certificación.
2. Certificado digital expedido por un prestador de servicios de certificación.
3. Llaves privada y pública generadas por una entidad certificadora autorizada.
4. Documento original previamente digitalizado.
5. Algoritmo de encriptación asimétrica, que cumpla con todos los estándares autorizados.
6. Proceso de conservación del mensaje, que cumpla con todos los estándares especificados y cuando la legislación así lo exija.¹⁷⁶

3.10. Alcance y valor probatorio de documentos con FEA(FIEL)

El Código de Comercio señala en el artículo 1205, que son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el

¹⁷⁵ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 225-227.

¹⁷⁶ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 227.

ánimo del juzgador acerca de los hechos controvertidos o dudosos, considerándose como pruebas entre otras, los mensajes de datos.

En esa tesitura, el artículo 1298-A, del citado código mercantil, da un tratamiento para la valoración de los mensajes de datos, al señalar que para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.

Así cuando la ley exija la forma escrita para los mensaje de datos, este supuesto se tendrá por cumplido siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente. Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido siempre que éste sea atribuible a dichas partes.

La Guía Jurídica de la Ley Modelo sobre Comercio Electrónico, establece diversos factores jurídicos que determinan la fiabilidad del método de creación de la firma, a saber:

- La perfección técnica del equipo utilizado por cada una de las partes.
- La naturaleza de su actividad comercial.
- La frecuencia de sus relaciones comerciales.
- El tipo y la magnitud de la operación.
 - La función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable.
 - La capacidad de los sistemas de comunicación.
 - La observancia de los procedimientos de autenticación establecidos por intermediarios.
 - La gama de procedimientos de autenticación que ofrecen los intermediarios.
 - La observancia de los usos y prácticas comerciales.

- La existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados.
- La importancia y el valor de la información contenida en el mensaje de datos.
- La disponibilidad de otros métodos de identificación y el costo de su aplicación.
- El grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento cuando se acordó el método como cuando se comunicó el mensaje de datos.
- Cualquier otro factor pertinente.¹⁷⁷

De lo anterior, se ha concluido que debe acreditarse que el método por el que se produjo el mensaje de datos, es confiable; lo cual, se logra en automático con una FIEL, al amparo de la cual, un prestador de servicios de certificación expide un certificado que acredita autenticidad, integridad, confidencialidad y no repudio del documento electrónico.

En ese orden de ideas, para que el juez conceda pleno valor probatorio a un mensaje de datos, se requiere presentar la prueba documental privada consistente en el archivo electrónico, junto con la constancia del prestador de servicios de certificación (documento que el prestador de servicios de certificación expide con base en el expediente electrónico); y, en su caso la pericial correspondiente.

Respecto de la prueba pericial, cabe mencionar que el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, en su artículo 4º, señala que la Secretaría de Economía (SE), integrará un padrón de profesionistas en las materias jurídica e informática que coadyuven a impulsar la utilización de los medios electrónicos en los actos de comercio. Para tal efecto, dicha Secretaría coordinará la capacitación de los referidos profesionistas, con el propósito de que éstos puedan ser designados peritos o árbitros en materia de prestación de servicios.

¹⁷⁷ *Ibidem*, p.p. 130.

En otras materias destacan las reformas al Código Federal de Procedimientos Civiles, en su adición del artículo 210-A; el cual, refiere al reconocimiento probatorio a la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología; asimismo, el artículo 776 de la Ley Federal del Trabajo, en el cual se señala como admisibles en el proceso, aquellos medios aportados por los descubrimientos de la ciencia; y, las relativas al Código Fiscal de la Federación, como es el caso de la utilización de la firma electrónica avanzada, cuando las disposiciones fiscales obliguen a presentar documentos (digitales).

3.11. La FEA(FIEL) en materia fiscal.

Después de una serie de reformas y adiciones al Código Fiscal de la Federación en los años 2004 y 2006, se dio cabida a los medios electrónicos, y por ende, el reconocimiento de la equivalencia funcional entre el documento tangible y los mensajes de datos, mediante el uso de una firma electrónica avanzada, así como los medios, formas y procedimientos para generar y utilizar ésta en materia fiscal.

Existen dos elementos que respaldan la fiabilidad de la firma electrónica avanzada; a saber: i). que los datos de creación hayan estado bajo el control exclusivo del firmante; y, ii). se cuente con el certificado digital.

Los *datos de creación* son códigos o claves criptográficas privadas, generados de manera secreta por el firmante, quien los utiliza para crear su firma electrónica al aplicar su llave privada, con el fin de lograr el vínculo entre dicha firma y su titular. Deberán ser tramitados por los contribuyentes (persona moral), ante el Servicio de Administración Tributaria (SAT). Cuando se traten de un contribuyente (persona física), ésta podrá tramitarlo ante dicha Administración, o bien, ante cualquier prestador de servicios de certificación (PSC) autorizado por el Banco de México.

El *certificado digital* es un mensaje de datos que identifica al dueño de una firma electrónica avanzada, es decir, confirma el vínculo entre el firmante y los datos de creación de una firma electrónica avanzada. Dicho certificado deberá encontrarse vigente, por lo que para efectos fiscales éste tiene una vigencia máxima de dos años, plazo que transcurre a partir de la fecha de expedición. Su titular podrá solicitar uno nuevo antes de que concluya el período de vigencia. Podrán cesar los efectos del certificado digital, entre otros, por: solicitud del firmante; resolución judicial o administrativa; transcurrido el plazo de dos años de vigencia del certificado; y, por riesgo sobre la confidencialidad de los datos de creación de la firma avanzada del SAT. El certificado digital deberá ser expedido por el Servicio de Administración Tributaria, tratándose de persona moral. Para el caso de persona física, el certificado digital es expedido por el SAT, o por un prestador de servicios de certificación autorizado por el Banco de México.

Bajo esa tesitura, el Código Fiscal de la Federación, dispone en el artículo 17-D, que cuando las disposiciones fiscales obliguen a presentar documentos, salvo los casos que establezcan una regla diferente; éstos deberán ser digitales y contener una firma electrónica avanzada del autor.

La firma electrónica avanzada deberá encontrarse amparada por un certificado vigente, que confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, el cual, como ya se ha dicho con antelación, deberá ser expedido por el Servicio de Administración Tributaria cuando se trate de personas morales, y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas.

Ello, trae como aparejado que un documento digital que contenga una firma electrónica avanzada, sea íntegro y, por tanto, pueda producir los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, así como el mismo valor probatorio.

Cabe afirmar, que no obstante el carácter obligatorio en materia fiscal, sobre la utilización de la firma electrónica avanzada, el legislador deja una excepción en el primer párrafo, parte final, del propio numeral 17-D citado, en el cual permite que las autoridades fiscales, mediante reglas de carácter general, autoricen el uso de otras firmas electrónicas, un ejemplo, la clave de identificación electrónica confidencial (CIEC), la cual como acertadamente lo consideran algunos autores, va a ser desplazada por la firma electrónica avanzada, en virtud de su confiabilidad y seguridad.

Pero, si la intención del legislador fue dar cabida a otro tipo de firma electrónica, considero que esta deberá tener la misma fiabilidad de la firma electrónica avanzada o mejor aún, mayor.

Por otra parte, se encuentran las autoridades registradoras centrales (ARC), las cuales son encargadas de certificar a su vez a los prestadores de servicios de certificación (PSC), para que puedan otorgar certificados de firma digital de todo tipo de documentos. Actualmente, las instituciones que ofrecen este servicio son:

- El Banco de México. ARC encargada de certificar a los prestadores de servicios de certificación del sector financiero.
- La Secretaría de Economía. Hace lo propio con los notarios, corredores y comerciantes.
- La Secretaría de la Función Pública. Certifica a las entidades gubernamentales como prestadoras de servicios de certificación.¹⁷⁸

3.12. Certificado digital.

Es un mensaje de datos firmado electrónicamente que vincula a una entidad identificada plenamente ante un prestador de servicios de certificación, con una llave pública que ha sido generada por dicho PSC.¹⁷⁹

¹⁷⁸ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 137-167..

¹⁷⁹ Cfr. *Ibidem*, 229.

Los certificados digitales están contenidos en archivos tipo *.cer, que cumplen con el estándar internacional CCITT (Comité Consultivo Internacional Telegráfico y Telefónico, por sus siglas en francés), establecido en el documento X.509 de la CCITT, y registran la información siguiente:

- a) Versión del formato del certificado. La versión predefinida es la 1. Si el certificado digital cuenta con los campos de Identificador único de emisor (Issuer unique identifier) o identificador único de asunto (Subject unique identifier), el valor de la versión debe ser 2. Si cuenta con una o más extensiones, la versión del formato del certificado debe ser 3.
- b) Número serial (Serial Number). Se trata de un valor numérico entero único dentro del dominio de una autoridad certificadora, que permite identificar un certificado sin duplicidad.
- c) Identificador de algoritmo de firma. El campo Signature algorithm identifier casi no se utiliza, ya que esta información se encuentra duplicada en el campo Firma.
- d) Nombre del emisor. Nombre de la autoridad certificadora que creó y firmó el certificado, en formato X.500.
- e) Período de validez. Indica el rango de fechas en el cual el certificado se considera vigente. Incluye la fecha de expedición del certificado digital y la fecha límite de validez.
- f) Nombre del sujeto. Nombre del usuario propietario del certificado.
- g) Información de clave pública del sujeto. Contiene la llave pública del propietario del certificado, un identificador del algoritmo para el cual se usará esta llave y algunos parámetros asociados.
- h) Identificador único de emisor. Sólo se utiliza cuando un nombre en formato X-509 se ha utilizado previamente por otras entidades. Se

trata de una cadena de bits que identifican de manera única al emisor.

- i) Extensiones. Son un conjunto de uno o más campos de extensiones. Cada extensión consiste en un identificador de extensión, un indicador de criticidad y un valor de extensión.
- j) Firma del emisor. Se incluye el resumen obtenido al aplicar la función Hash a los campos anteriores del certificado; dicho resumen es incluido una vez que se ha encriptado con la llave privada de la autoridad certificadora. Este campo también incluye el identificador del algoritmo de la firma.¹⁸⁰

En la práctica se emiten cuatro tipos de certificados digitales:

1. Certificado para persona física. Permiten a los usuarios realizar intercambios seguros de mensajes con otras personas o servicios en línea.
2. Certificado para persona moral. Permiten a las personas morales realizar intercambios seguros de mensajes; éstos se emiten al representante de una persona moral, quien es requisito indispensable que cuente con su certificado como persona física.
3. Certificado de dominio. Permite generar confianza entre los usuarios de un sitio web, ya que garantiza al visitante que dicho sitio ha sido validado por un PSC. Actualmente, sólo se valida el perfil legal y comercial de la empresa que mantiene un sitio web, al implementar un certificado SSL (Secure Socket Layer) de 128 bits. El protocolo SSL es el mecanismo más utilizado y aceptado para garantizar la autenticación, integridad y confidencialidad de los datos que se transmiten entre el cliente y el servidor a través de Internet, ya que permite la encriptación de dichos datos y certifica al propietario de

¹⁸⁰ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, págs. 229 y 230.

dicho servidor. Ha sido un gran éxito la facilidad de implementación a través de un certificado que se instala en el servidor web.

4. Certificado de código. Son certificados que permiten validar porciones de código de programación autenticando a su autor, de modo que el sistema del usuario sea capaz de detectar un riesgo de seguridad debido al origen desconocido de ciertos códigos. En el supuesto de que en un segmento del código represente un riesgo, el navegador de Internet mostrará un cuadro de diálogo al usuario donde éste decide si confía en el origen de dicho código para que pueda ser ejecutado, de lo contrario el código será rechazado y no se ejecutará.¹⁸¹

Las entidades que interviene en la emisión de certificados integran una infraestructura jerárquica, lo cual garantiza un proceso seguro y confiable; de las que se encuentran:

- a) Fedatario Público. Da fe de la identidad del solicitante, revisa la documentación para verificar la identidad y remite el requerimiento de certificado a una autoridad registradora.
- b) Autoridad registradora. Emite un precertificado y lo envía a la autoridad certificadora, procesa el requerimiento de certificado y valida la generación de las llaves; revisa que no haya duplicidad en las llaves.
- c) Autoridad certificadora (AC). Emite el certificado definitivo, posee un certificado raíz con llaves encriptadas y custodiadas por un conjunto de otras AC, de tal forma que todas las entidades que intervienen están plenamente identificadas y soportadas por un esquema redundante. Esto se logra utilizando hardware criptográfico FIPS 140-1 nivel 3.

En la práctica actual es posible que una entidad ejerza la función de cada uno

¹⁸¹ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, págs. 230-232.

de los tres niveles jerárquicos o de dos de ellos. En México, el SAT, en su calidad de prestador de servicios de certificación para las personas morales, es la entidad que asume la calidad de fedatario público y autoridad registradora. En tratándose de personas físicas, es un prestador de servicios de certificación autorizado por el Banco de México quien ejerce dicha función.¹⁸²

3.13. Sello digital

Es un mensaje electrónico que acredita que un documento digital fue recibido por la autoridad correspondiente; es decir, cuando los contribuyentes remitan un documento digital a las autoridades fiscales, recibirán el acuse de recibo que contenga el sello digital.

El sello digital se encuentra sujeto a la misma regulación aplicable al uso de una firma electrónica avanzada, por lo que también requiere de un certificado digital para dar seguridad al mismo.

El sello digital identifica a la dependencia que recibió el documento y se presumirá, salvo prueba en contrario, que el documento digital fue recibido en la hora y fecha que se consignen en el acuse de recibo mencionado. En esa tesitura, el Servicio de Administración Tributaria establecerá los medios para que los contribuyentes puedan verificar la autenticidad de los acuses de recibo con sello digital.

El sello digital, al que también se le conoce como *cadena digital*, tiene las características siguientes:

- Es infalsificable.
- No es reciclable (es único por documento).
- Cualquier alteración de la información es detectable.
- No puede ser repudiado.¹⁸³

¹⁸² Cfr. *Ibidem*, p.p. 232 y 233.

¹⁸³ León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit. p.p. 237.

En la generación de un sello digital se utilizan los siguientes algoritmos:

- **MD5.** Es la función Hash para crear un resumen digital:
- **RSAPrivateEncrypt.** Utiliza la llave privada del emisor para encriptar el resumen digital del mensaje producido con el algoritmo MD5.
- **RSAPublicDecrypt.** Utiliza la llave pública del emisor para desencriptar el resumen digital del mensaje.¹⁸⁴

Los elementos utilizados en la generación de un sello digital son a saber:

- a) Cadena original, que es un comprobante fiscal digital.
- b) Certificado para sellos digitales y sus correspondientes llaves pública y privada.
- c) Algoritmos de criptografía de llave pública para firma electrónica avanzada.
- d) Especificaciones de conversión de la firma electrónica avanzada a Base 64.¹⁸⁵

Por su parte, el procedimiento para el sellado digital de una cadena original o comprobante digital, es el siguiente:

1. Se aplica la función Hash MD5 al mensaje original que contiene todos los datos del comprobante o acuse de recibo. Esta función genera un resumen digital de 128 bits (16 bytes) en todos los casos, sin importar el tamaño de la cadena original. Se hace la observación, que en las funciones Hash una alteración de la cadena original, por mínima que sea, provoca un resumen digital totalmente diferente, razón por la cual este mecanismo se considera totalmente seguro.

¹⁸⁴ Cfr. *Ibidem*, p.p. 237 y 238.

¹⁸⁵ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit, p.p. 238.

2. El resumen digital que resulta de la función anterior, se encripta por medio del algoritmo asimétrico RSA utilizando la llave privada correspondiente al certificado de sello digital del emisor. El resultado de dicha encriptación es una cadena binaria que no necesariamente puede imprimirse de manera directa.
3. Para imprimir la cadena binaria, primero debe convertirse a una cadena de caracteres imprimibles, utilizando el método Base 64. Este método consiste en la agrupación de cada 6 bits de la secuencia para asociarlos a un elemento de un conjunto de 64 caracteres imprimibles. Dado que 6 bits pueden expresar los números del 0 al 63, a cada elemento del conjunto se le asigna uno de estos valores. Este procedimiento de expresión de cadenas binarias incrementa el tamaño de las cadenas imprimibles en 25% con respecto de la original, lo cual da como resultado una cadena de 172 caracteres imprimibles utilizando una llave de 1024 bits.¹⁸⁶

La codificación en Base 64, así como su decodificación, se lleva a cabo tomando los bloques de izquierda a derecha. El conjunto de elementos que únicamente pueden ser asignados en cada bloque de 6 bits está integrado por los caracteres siguientes:¹⁸⁷

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, +, /

En esa tesitura, a los caracteres les corresponden los valores del 0 al 64. Para realizar la conversión inversa, es decir, de Base 64 a la cadena original, se agrupan 4 caracteres a la vez de izquierda a derecha; estos caracteres representan un juego de 24 bits (4 caracteres x 6 bits cada uno) y se tratan como un juego de 3 caracteres binarios de 8 bits cada uno. La operación se repite hasta completar una cadena imprimible.¹⁸⁸

¹⁸⁶ Ídem.

¹⁸⁷ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit. p.p. 239.

¹⁸⁸ Ídem

Un ejemplo de sello digital es el siguiente:¹⁸⁹

Tnhf45G94eITpoQW456nkGT/nh+30aWdQ234lm9jhf54D5h9kmn76gDkjMo98RF3
AyQyN897uy3vNi87hsQW326g549jhgXklA0tr43wsfvcGH89J+mjQW234tjhnu764
NJMK9+ujdQW/hb76ytAWSKOL98ujbhgERFD43kj2+J=

El código postrado representa un resumen digital ya encriptado correspondiente a un acuse de recibo, además ha sido procesado con el método Base 64 para que sea posible su impresión.¹⁹⁰

4. Prestadores de servicios de certificación en materia mercantil.

El Código de Comercio establece en el artículo 89, que el prestador de servicios de certificación, es la persona o institución pública que presta servicios relacionados con firmas electrónicas y que expide los certificados, en su caso.

Pueden ser prestadores de servicios de certificación, previa acreditación de la Secretaría de Economía, los siguientes:

- a) Los notarios públicos y corredores públicos.
- b) Las personas morales de carácter privado.
- c) Las instituciones públicas, conforme a las leyes que les son aplicables.

Un punto que cabe destacar en esta materia, fue la controversia constitucional en Colombia sobre la Ley 527 de 1999, en lo relativo a la expedición de certificados que tienen como función los prestadores de servicios de certificación, al argüir la demandante que dicha función únicamente corresponde al notario público; el resultado de esta controversia fue que se declaró la no inconstitucionalidad de dicha Ley, al concluirse entre otros puntos, que la actividad de certificación es un servicio de índole eminentemente técnico.

¹⁸⁹ Ídem.

¹⁹⁰ Ídem.

En nuestro país, se señala que la facultad de expedir certificados no conlleva fe pública por sí misma; así los notarios y corredores públicos pueden llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información; ello, en observancia al artículo 100 del Código de Comercio.

En ese sentido, la Secretaría de Economía es la encargada de acreditar a los prestadores de servicios de certificación, éstos deberán notificar a aquella la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad. Si la Secretaría citada no ha resuelto respecto a la petición del solicitante para ser acreditado como prestador de servicio de certificación dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.

4.1. Requisitos para obtener acreditación como PSC.

Para que las personas que prevé el artículo 100 del Código de Comercio, puedan ser prestadores de servicios de certificación, deben cumplir los siguientes requisitos:

- a) Solicitar a la Secretaría de Economía la acreditación como prestador de servicios de certificación.
- b) Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad.
- c) Contar con procedimientos definidos y específicos para la tramitación del certificado, y medidas que garanticen la seriedad de los certificados emitidos, la conservación y consulta de los registros.
- d) Quienes operen o tengan acceso a los sistemas de certificación de los prestadores de servicios de certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya

merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

- e) Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la SE.
- f) Establecer por escrito su conformidad para ser sujeto a auditoría por parte de la SE.
- g) Registrar su certificado ante la SE.

El cumplimiento de estos puntos serán de observancia de la Secretaría de Economía, quien podrá requerir a los prestadores de servicios de certificación que comprueben el cumplimiento de los mismos.

4.2. Acreditación de los PSC conforme al reglamento del Código de Comercio en materia de PSC.

En apego al artículo 5º, del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, los interesados en obtener la acreditación como prestador de servicios de certificación deberán:

- a) Presentar la solicitud de acreditación en los formatos que determine la Secretaría de Economía. En caso de los **notarios o corredores públicos**, copia certificada de la patente, título de habilitación o documento que en términos de la legislación de la materia les acredite estar en ejercicio de la fe pública. Las **instituciones públicas** deberán presentar copia certificada del instrumento jurídico de su creación o, en su caso, copia certificada de su acta constitutiva, de conformidad con las disposiciones jurídicas aplicables. En caso de las **personas morales**, copia certificada de su acta constitutiva, póliza u otro instrumento público, que acredite su constitución de acuerdo con las leyes mexicanas, y que su objeto social sea los

siguientes: i). Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica; ii). Comprobar la integridad y suficiencia del mensaje de datos del solicitante y verificar la firma electrónica de quien realiza la verificación; iii). Llevar a cabo registros de los elementos de identificación de los firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las firmas electrónicas avanzadas y emitir el certificado; y, iv). Cualquier otra actividad no incompatible con las anteriores.

- b) Comprobar que se cuenta al menos con los siguientes elementos: i). **Humanos.** Un profesional jurídico, un profesional informático y cinco auxiliares de apoyo informático; ii). **Materiales.** Espacio físico apropiado para la actividad, controles de seguridad, accesos y perímetros de seguridad física, medidas de protección, así como con las políticas necesarias para garantizar la seguridad del área. iii). **Económicos.** Capital que comprenderá al menos el equivalente a una cuarta parte de la inversión requerida para cumplir con los elementos humanos, tecnológicos y materiales, y un seguro de responsabilidad civil cuyo monto será determinado por la SE con base en el análisis de las operaciones comerciales y mercantiles en que sean utilizados los certificados y no será menor al equivalente a treinta veces el salario mínimo general diario vigente en el Distrito Federal correspondiente a un año; iv). **Tecnológicos.** Consistentes en análisis y evaluación de riesgos y amenazas, infraestructura informática, equipo de cómputo y software, política de seguridad de la información, plan de continuidad del negocio y recuperación ante desastres, plan de seguridad de sistemas, estructura de certificados, estructura de la lista de certificados revocados, sitio electrónico, procedimientos que informen de las características de los procesos de creación y verificación de firma electrónica avanzada, política de certificados, declaración de prácticas de certificación, modelos de las autoridades certificadora y registradora, y plan de administración de claves.

- c) Contar con procedimientos claros y definidos de conformidad con las Reglas Generales que emita la Secretaría de Economía.
- d) Adjuntar a la solicitud una carta suscrita por cada persona física que pretenda operar o tener acceso a los sistemas que utilizará en caso de ser acreditado, donde dicha persona manifieste bajo protesta de decir verdad y advertido de las penas en que incurren los que declaren falsamente ante una autoridad distinta a la judicial, de que no fue condenado por delito contra el patrimonio de las personas y mucho menos inhabilitado para el ejercicio de la profesión, o para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.
- e). Contar con una póliza de fianza por el monto y condiciones que se determinan en el presente Reglamento y en las Reglas Generales que al efecto expida la Secretaría de Economía.
- f) Acompañar a su solicitud, escrito de conformidad para ser sujeto de auditoría por parte de la SE en todo momento, para que ésta verifique el cumplimiento de los requisitos para obtener y mantener la acreditación como prestador de servicios de certificación. Cuando el interesado pretenda que sus datos de creación de firma electrónica permanezcan en resguardo fuera del territorio nacional, deberá solicitarlo a la Secretaría citada. En este caso, el interesado manifestará por escrito su conformidad de asumir los costos que impliquen a la Secretaría de Economía el traslado de su personal para efectuar sus auditorías.
- g) Registrar ante la SE su certificado, en los términos que establece el presente Reglamento.

4.3. Certificado de acreditación como PSC.

Una vez que se haya resuelto favorablemente el otorgamiento de certificado de acreditación a prestador de servicio de certificación, se observará lo siguiente:

- a) La Secretaría de Economía publicará en el Diario Oficial de la Federación las acreditaciones que otorgue, dentro de los treinta días siguientes a la resolución que determine su procedencia. La misma situación se observará en caso de que la SE no resuelva la solicitud del interesado en el plazo de la fracción anterior.
- b). La SE establecerá en las Reglas Generales las condiciones a que se sujetará la fianza que otorgarán los interesados que obtengan su acreditación, previo al inicio de operaciones como prestadores de servicios de certificación. Los interesados contarán con un plazo de diez días a partir de que se haya autorizado la procedencia de la acreditación, para obtener de compañía debidamente autorizada la fianza que deberán de presentar ante la SE.
- c) La SE una vez que reciba la fianza verificará que contenga lo señalado en el Código de Comercio, en este Reglamento y en las Reglas Generales que al efecto expida y, hecho lo anterior, procederá a expedir el certificado respectivo al interesado y lo registrará a efecto de que éste pueda iniciar operaciones.
- d) La SE como autoridad certificadora y registradora, deberá comprobar la identidad del prestador de servicios de certificación o su representante, para que éste pueda generar sus datos de creación de firma electrónica.
- e) El prestador de servicios de certificación o su representante no podrán revelar los datos de creación de firma electrónica que correspondan a su propio certificado y en todo caso serán responsables de su mala utilización.
- f) El acreditado deberá notificar por escrito a la SE la fecha en que inicie su actividad como prestador de servicios de certificación. La notificación podrá efectuarse dentro de los 45 días naturales siguientes al comienzo de dicha actividad.
- g) El certificado tendrá una vigencia de diez años.

4.4. Contratos de certificación de autoridad.

Para dar fiabilidad y seguridad a los contratos por medios electrónicos, así como los relacionados con la prueba de existencia de los negocios jurídicos celebrados por Internet, se han creado las PSC, quienes mediante un contrato de comercio electrónico de servicios de certificación con el usuario, establecen las bases y condiciones que rigen el intercambio de mensajes de datos que el cliente generará con terceros.¹⁹¹

En ese sentido, los prestadores de servicios de certificación definen las medidas de seguridad para proteger la información intercambiada contra su posible interceptación o uso por terceros. La medida que asegura la identidad del emisor del mensaje de datos es la certificación, la cual se obtiene mediante la obtención de servicios de certificación de autoridad prestados por personas de derecho privado y autoridades gubernamentales, quienes ofrecen el servicio a los usuarios que desean certificar su identidad en la red.¹⁹²

Ello, ha dado como resultado que las partes de contratos a celebrarse por mensajes de datos, pueden convenir que en la celebración de sus contratos por Internet se cuente con la certificación de autoridad, conforme a la cual se certifica que una clave de encriptación pública específica se utiliza para una persona en particular. Este proceso se lleva a cabo través de un certificado de identidad electrónico, que se emite una vez que se presentan a la autoridad certificadora los documentos idóneos que comprueban la identidad del usuario o emisor. Dicha identidad queda certificada mediante la emisión y publicación de un certificado accesible por Internet, el cual, emite la autoridad certificadora una vez que ha comprobado la identidad. Con esta medida el usuario o emisor, queda obligado a preservar la confidencialidad de la contraseña de acceso a su clave privada y a informar de manera pronta a la autoridad certificadora cualquier quebranto de la seguridad de su sistema de cómputo que pudiera comprometer dicha confidencialidad; al tiempo que le proporciona la

¹⁹¹ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit. p.p. 118.

¹⁹² Ídem.

seguridad de que los mensajes de datos enviados y recibidos por dicho usuario o emisor son auténticos y, por consiguiente, los contratos que celebra son ciertos y eficaces, y como consecuencia, pueden producir efectos jurídicos.¹⁹³

4.5. Certificados digitales en materia mercantil.

Como lo señala el Código de Comercio, el certificado es todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de firma electrónica.

En ese sentido, una FIEL amparada por un certificado vigente, sustituye a la firma autógrafa del firmante, lo que garantiza la integridad del documento y produce los mismos efectos que las leyes otorgan a los documentos con firma autógrafa.¹⁹⁴

Se puede definir el certificado digital como el conjunto de información única, almacenada y procesada electrónicamente que identifica, verifica y autentica a un usuario como parte del proceso de generación de su firma electrónica. Es un documento de identidad del firmante en el ambiente cibernético. Se compone de tres elementos: la llave pública, la llave privada y la firma electrónica; lo que permite al titular lo siguiente:¹⁹⁵

- a) Identificarse ante terceros e informar sobre su capacidad para actuar en representación de una persona moral.
- b) Firmar documentos electrónicamente con el mismo valor legal que la firma manuscrita, de tal forma que se garantice la autenticidad de los compromisos adquiridos.
- c) Proteger la información transmitida garantizando que no haya sido manipulada o leída por terceros, y por tanto, proteger la integridad y

¹⁹³ Cfr. León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, ob. cit. p.p. 119.

¹⁹⁴ Cfr. *Ibidem*, p.p. 120.

¹⁹⁵ *Ídem*.

confidencialidad de los contenidos.

4.6. Contenido del certificado digital en materia comercial conforme al Código de Comercio

Según el artículo 108 del Código de Comercio, los certificados para ser considerados válidos, deberán contener:

- a) La indicación de que se expiden como tales
- b) El código de identificación único del certificado.
- c) La identificación del prestador de servicios de certificación que expide el certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría de Economía.
- d) Nombre del titular del certificado.
- e) Período de vigencia del certificado.
- f) La fecha y hora de la emisión, suspensión, y renovación del certificado.
- g) El alcance de las responsabilidades que asume el prestador de servicios de certificación.
- h) La referencia de la tecnología empleada para la creación de la firma electrónica.

4.7. El certificado conforme al Reglamento del Código de Comercio en materia de PSC.

El Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, establece en sus numerales 15 al 20, lo siguiente:

- a) El prestador de servicios de certificación deberá proporcionar a la Secretaría de Economía su dirección electrónica, la que deberá incluir en

cada certificado que expida para verificar en forma inmediata su validez, suspensión o revocación. Esta dirección se utilizará por la SE para agregarla a un dominio propio de consulta en línea, a través del cual la parte que confía podrá cerciorarse del estado que guarda cualquier certificado emitido por un prestador de servicios de certificación.

- b) Los prestadores de servicios de certificación deberán enviar en línea, mediante el procedimiento que establezcan las Reglas Generales que expida la SE, una copia de cada certificado que generen. Los certificados enviados se resguardarán por la SE bajo el más estricto mecanismo de seguridad física y lógica.
- c) Los datos de acreditación ante la Secretaría de Economía, que contendrán los certificados que expidan los prestadores de servicios de certificación, incluirán al menos para ser considerados válidos: i). el nombre, denominación o razón social y domicilio del prestador de servicios de certificación; ii). la dirección electrónica donde podrá verificarse la lista de certificados revocados a prestadores de servicios de certificación, y iii). los demás que, en atención al avance tecnológico, se establezcan en las Reglas Generales que expida la SE. El prestador de servicios de certificación deberá notificar a la Secretaría en comento cualquier cambio que pretenda efectuar respecto de los datos referidos en los puntos anteriores.
- d) La Secretaría de Economía determinará en las Reglas Generales que expida, la utilización de un sello de tiempo para asegurar la fecha y hora de la emisión, suspensión y revocación del certificado.
- e) La emisión, registro y conservación de los certificados por parte de los prestadores de servicios de certificación se efectuará en territorio nacional. La Secretaría de Economía, a través de las Reglas Generales preverá los mecanismos que garanticen que los certificados emitidos por los

prestadores de servicios de certificación, en ningún caso, contengan elementos que puedan generar confusión en la parte que confía.

- f) La Secretaría de Economía podrá autorizar el resguardo de los datos de creación de firma electrónica del prestador de servicios de certificación fuera del territorio nacional. En este caso, el prestador de servicios de certificación asumirá los costos que impliquen a dicha Secretaría el traslado de sus servidores públicos para efectuar las visitas de verificación (auditorías).

4.8. Obligaciones de los PSC en la FEA(FIEL).

El artículo 104, del Código de Comercio, establece que los prestadores de servicios de certificación deben cumplir las siguientes obligaciones:

- a) Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante.
- b) Poner a disposición del firmante los dispositivos de generación de los datos de creación y de verificación de la firma electrónica.
- c) Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad.
- d) Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología

y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del destinatario y de las personas que lo soliciten cuando así lo autorice el firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría de Economía.

- e) Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación.
- f) En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo a la Secretaría de Economía a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos.
- g) Asegurar las medidas para evitar la alteración de los certificados y mantener la confidencialidad de los datos en el proceso de generación de los datos de creación de la firma electrónica.
- h) Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el destinatario.
- i) Proporcionar medios de acceso que permitan a la parte que confía en el certificado determinar lo siguiente: i). La identidad del prestador de servicios de certificación; ii). Que el firmante nombrado en el certificado tenía bajo su control el dispositivo y los datos de creación de la firma en el momento en que se expidió el certificado; iii). Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado; iv). El método utilizado para identificar al firmante; v). Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado; vi). Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el prestador de servicios de certificación; vii). Si existe un medio para que el firmante dé aviso al prestador de servicios de certificación de que los datos de

creación de la firma han sido de alguna manera controvertidos; y, viii). Si se ofrece un servicio de terminación de vigencia del certificado.

4.9. Obligaciones del titular del certificado.

Al respecto, el artículo 99 del Código de Comercio, señala que el firmante deberá:

- a) Cumplir las obligaciones derivadas del uso de la firma electrónica.
- b) Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los datos de creación de la firma.
- c) Cuando se emplee un certificado en relación con una firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el certificado, con su vigencia, o que hayan sido consignadas en el mismo, son exactas. El firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en este apartado.
- d) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia.

4.10. Del reconocimiento de certificados y firmas electrónicas extranjeras.

Se ha adoptado el reconocimiento del certificado y de la firma electrónica extranjeros, sin considerarse el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica, ni el lugar en que se encuentre el establecimiento del prestador de servicios de certificación o del firmante.

El artículo 114 del Código de Comercio, establece que el certificado fuera de la República Mexicana producirá los mismos efectos jurídicos que un certificado expedido en la República Mexicana, si presenta un grado de fiabilidad equivalente a los contemplados por el propio código.

Por ende, la firma electrónica creada o utilizada extranjera, producirá los mismos efectos jurídicos en la misma que una firma electrónica creada o utilizada en la República Mexicana, si presenta un grado de fiabilidad equivalente.

Para efecto de determinar dicho grado de fiabilidad, se toman en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente; en esa tesitura, cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

5. Criterio e interpretación actual del Código de Comercio sobre la firma electrónica, y derecho comparado.

México recoge los lineamientos sobre la firma electrónica plasmados en la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas. En abril de 1999 el Partido Acción Nacional presentó la iniciativa del texto de la Ley Modelo de UNCITRAL y en marzo de 2000, el Partido Revolucionario Institucional presentó la iniciativa de texto simplificado y aumentado con Protección al Consumidor, lo que motivó que en 29 de abril de ese año, se aprobara un Decreto mediante el cual se reformaron y se adicionaron disposiciones al Código Civil Federal, Código Federal de Procedimientos Civiles, Código de Comercio y a la Ley Federal de Protección al Consumidor.

Actualmente, si bien son abundantes los criterios de la Suprema Corte de Justicia de la Nación, así como de los Tribunales Colegiados, sobre temas como los medios electrónicos, declaración presentada a través de éstos, información por medio de Internet, valor probatorio de los documentos electrónicos, etcétera; no ha sido así

sobre la firma electrónica; no obstante, creo que dado que esta materia es novedosa, conforme se tramiten y resuelvan ante los órganos jurisdiccionales más asuntos cuyo fondo incida sobre la utilización de la firma electrónica, emanaran más criterios, mismos que darán a los justiciables certeza jurídica, y orientaran al juzgador para resolver de manera pronta, completa e imparcial los asuntos que sobre esta materia se ventilen.

Entre los criterios actuales sobre esta materia, destacan los siguientes:

- **Localización:** Novena Epoca, Instancia: Tribunales Colegiados de Circuito, Fuente: Semanario Judicial de la Federación y su Gaceta, XIX, Enero de 2004, Página: 1492, Tesis: I.1o.A.120 A, Tesis Aislada, Materia(s): Administrativa.

“CONTRIBUCIONES. LA COPIA SIMPLE DEL COMPROBANTE DE PAGO POR MEDIOS ELECTRÓNICOS OBTENIDA MEDIANTE IMPRESORA, FAX O CUALQUIER OTRO MEDIO ANÁLOGO ES APTA PARA ACREDITAR EL ACTO DE APLICACIÓN DEL ARTÍCULO TERCERO TRANSITORIO DE LA LEY DEL IMPUESTO SOBRE LA RENTA VIGENTE EN EL AÑO DOS MIL TRES. Del artículo 31, segundo párrafo, del Código Fiscal de la Federación y de la regla 2.9.17. de la Resolución Miscelánea Fiscal vigente en febrero del año dos mil tres se desprende que cuando los contribuyentes realicen el cumplimiento de sus deberes fiscales por medios electrónicos, no es obligatorio que presenten la declaración correspondiente en las formas aprobadas por la Secretaría de Hacienda y Crédito Público, en virtud de que los contribuyentes podrán presentar la declaración en las citadas formas para obtener el sello o impresión de la máquina registradora, lo que significa que se está en presencia de una facultad o derecho del gobernado que puede o no ejercer y no de un deber; en igual forma, es una facultad de éste obtener copia certificada de las declaraciones presentadas por medios electrónicos. Ahora bien, el pago de contribuciones por medios electrónicos constituye un instrumento para facilitar el cumplimiento de las obligaciones fiscales de los gobernados y la pronta y eficaz recaudación, cuya forma de operar implica que los causantes tengan una clave de acceso al sistema tributario cuando realicen pagos por transferencia electrónica, en tanto que la institución financiera proporcionará el sello digital. El concepto del "equivalente funcional" entre los documentos consignados en papel y aquellos consignados por vía electrónica tiene por objeto establecer una serie de características numéricas y criptográficas que identifican a la persona y aprobar la información que aparece en el mensaje, de ahí que la reproducción de la información mediante impresora, fax o cualquier otro medio análogo, que naturalmente se reduce a copia simple, no significa, en modo alguno, que carezcan de valor probatorio para demostrar el acto de aplicación del artículo tercero transitorio de la Ley del Impuesto sobre la Renta,

vigente en el año dos mil tres, reclamado, por el simple hecho de que consten en copia simple, antes bien, son confiables partiendo de la base de los fines del artículo 31 del ordenamiento citado, que sirvió de fundamento para generar la información electrónica, en virtud de que la seguridad de la operación se encuentra en la clave digital que es original, administrada con los demás datos como son el registro federal de contribuyentes, la fecha de pago, el número de cuenta, el número de operación, el periodo, el impuesto y la cantidad que se paga y, en todo caso, el fisco federal, de no estar de acuerdo con su contenido, está en posibilidad de impugnarlo, y si no lo hizo, tal omisión se traduce en su aceptación tácita para todos los efectos legales, porque la presentación de una declaración escrita para obtener el sello oficial en original o la impresión en ella de la máquina registradora, después de haber realizado el pago o cumplimiento de obligaciones fiscales por medios electrónicos, es una facultad o derecho del gobernado que puede o no ejercer a su juicio, porque no se trata de un deber, una obligación. Por tanto, la fuerza probatoria deriva de la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser exigida para su ulterior consulta, de conformidad con lo dispuesto por el artículo 210-A del Código Federal de Procedimientos Civiles, aplicado supletoriamente en términos del artículo 2o. de la Ley de Amparo, y no de la aplicación dogmática de una regla general de que las copias simples carecen, por sí mismas, de valor, por el hecho de que el sello digital se encuentra en una copia simple obtenida de impresora, fax, entre otros, ya que los avances tecnológicos, a nivel mundial, trajeron como resultado que el legislador introdujera los medios electrónicos para crear, modificar, extinguir o cumplir obligaciones, según se advierte de los artículos 31 del código tributario, 89 a 114 del Código de Comercio, 188 y 210-A del Código Federal de Procedimientos Civiles, entre otros ordenamientos, que establecen excepciones a la regla general citada. Por consiguiente, si al realizar el pago provisional del impuesto sustitutivo del crédito al salario que le corresponde, el acuse referido es el único documento que obtuvo el particular al realizar su pago de esa forma, es claro que si las autoridades hacendarias no lo objetaron, por razones de lealtad procesal, de probidad y buena fe frente al Juez, quien debe evitar que se trastoquen dichos valores, debe considerarse apto y suficiente para demostrar el pago de referencia y, por ende, el acto concreto de aplicación de la norma tildada de inconstitucional y su interés jurídico para cuestionarla; con mayor razón si la quejosa, en el escrito de demanda, manifestó bajo protesta de decir verdad que la copia simple en la que consta la **firma electrónica**, es real, sin perjuicio de las responsabilidades que le pudieran resultar, en el supuesto de que llegara a faltar a la verdad, sobre todo si se toma en cuenta que la autoridad fiscal se abstuvo de cuestionar la veracidad de la firma electrónica, no obstante que cuenta con la base de datos que contiene los sellos digitales y las firmas electrónicas.”(resalto)

- **Localización:** Novena Epoca, Instancia: Tribunales Colegiados de Circuito, Fuente: Semanario Judicial de la Federación y su Gaceta, XIII, Junio de 2001, Página: 677, Tesis: VII.1o.A.T.48 A, Tesis Aislada, Materia(s): Administrativa:

“AUTORIDADES ADUANERAS. SON COMPETENTES PARA VERIFICAR EL CUMPLIMIENTO DE LAS REGULACIONES Y RESTRICCIONES NO ARANCELARIAS DE MERCANCÍA DE IMPORTACIÓN, EN EL PUNTO DE SU ENTRADA O SALIDA, PREVISTAS EN LA NOM-015/1-SCFI/SSA-1994. La correcta interpretación de los artículos 36, fracción I, inciso c), de la Ley Aduanera y 26 de la Ley de Comercio Exterior, el primero de los cuales establece: "Artículo 36. Quienes importen o exporten mercancías están obligados a presentar ante la aduana, por conducto de agente o apoderado aduanal, un pedimento en la forma oficial aprobada por la secretaría. En los casos de las mercancías sujetas a regulaciones y restricciones no arancelarias cuyo cumplimiento se demuestre a través de medios electrónicos, el pedimento deberá incluir la **firma electrónica** que demuestre el descargo total o parcial de esas regulaciones o restricciones. Dicho pedimento se deberá acompañar de: I. En importación: ... c) Los documentos que comprueben el cumplimiento de las regulaciones y restricciones no arancelarias a la importación, que se hubieran expedido de acuerdo con la Ley de Comercio Exterior, siempre que las mismas se publiquen en el Diario Oficial de la Federación y se identifiquen en términos de la fracción arancelaria y de la nomenclatura que les corresponda conforme a la tarifa de la Ley del Impuesto General de Importación.", y el segundo prescribe: "Artículo 26. En todo caso, la importación, circulación o tránsito de mercancías estarán sujetos a las normas oficiales mexicanas de conformidad con la ley de la materia. ... La secretaría determinará las normas oficiales mexicanas que las autoridades aduaneras deban hacer cumplir en el punto de entrada de la mercancía al país. ...", permite establecer que las autoridades aduaneras son competentes para verificar el cumplimiento de las obligaciones no arancelarias al levantar el acta de inicio de procedimiento administrativo y reconocimiento aduanero de mercancías que ingresan al país, a que se refiere la Norma Oficial Mexicana NOM-015/1-SCFI/SSA-1994, "Seguridad e información comercial en juguetes-seguridad de juguetes y artículos escolares. Límites de biodisponibilidad de metales en artículos recubiertos con pinturas y tintas. Especificaciones químicas y métodos de prueba.”(resalto)

- **Localización:** Novena Epoca, Instancia: Segunda Sala, Fuente: Semanario Judicial de la Federación y su Gaceta, XXVI, Agosto de 2007, Página: 638, Tesis: 2a. XCVII/2007, Tesis Aislada, Materia(s): Constitucional, Administrativa.

“FIRMA ELECTRÓNICA AVANZADA. EL HECHO DE QUE EL CÓDIGO FISCAL DE LA FEDERACIÓN NO ESTABLEZCA SU DEFINICIÓN NO VIOLA LA GARANTÍA DE LEGALIDAD. El artículo

17-D del Código Fiscal de la Federación establece que cuando las disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos previstos en el propio precepto, y que para esos efectos deberá contarse con un certificado que confirme el vínculo entre un firmante y los datos de creación de una "**firma electrónica avanzada**", expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas, mediante el cumplimiento de ciertos requisitos, entre ellos, el de la comparecencia del interesado o de su apoderado o representante legal en caso de personas morales, con la finalidad de acreditar su identidad. De lo anterior se concluye que no se viola la garantía de legalidad contenida en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, por el hecho de que el Código Fiscal de la Federación no establezca una definición particular de lo que debe entenderse por "**firma electrónica avanzada**", pues del indicado numeral 17-D se advierte el propósito perseguido con ésta, el cual, además de identificar al emisor de un mensaje como su autor legítimo, como si se tratara de una firma autógrafa, garantiza la integridad del documento produciendo los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio; lo anterior, en razón de que la firma electrónica avanzada está vinculada a un certificado expedido por una autoridad, en este caso, por el Servicio de Administración Tributaria, en el que constan los datos del registro respectivo.”(resalto)

En términos de derecho comparado el tema de la firma electrónica ha tomado relevancia en diversas naciones, lo que ha motivado a legislar sobre esta materia. A través de la decisión de invertir esfuerzo y ver hacia siempre adelante, se han integrado actualmente una gran mayoría de las naciones que apuestan por el desarrollo tecnológico y económico; entre otros, se encuentran: Estados Unidos de América, Argentina, Colombia, Chile, Ecuador, Panamá, Perú, Italia, España, México, etcétera.

Estados Unidos de América.

En mayo de 1995 fue emitida la primera ley sobre firmas digitales por el Estado de Utah y es conocida como “Utah Digital Signature Act”. El Comité de Seguridad de la Información de la División de Comercio Electrónico, de la American Bar Association, emitió en agosto de 1996, la “Guía de Firmas Digitales”. El 15 de agosto de 1997 en la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme, elaboró el borrador de lo que será la “Uniform Electronic Transactions

Act”, que fue aprobada el 30 de julio de 1999. El 30 de junio de 2000, se emitió la “Electronic Signatures in Global and National Commerce Act”.¹⁹⁶

Argentina.

El 17 de marzo de 1997 el Sub-Comité de Criptografía y Firma Digital, dependiente de la Secretaría de la Función Pública emitió la resolución 45/97. En marzo de 1999, se encargó un grupo de juristas (Comisión creada por Decreto 685/95) la redacción de un Proyecto de Código Civil que también abarcara las materias electrónico comerciales.¹⁹⁷

Colombia.

Se crea la Ley 527 de 1999, en la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.¹⁹⁸

Chile.

El 10 de junio de 1999, el presidente Eduardo Frei presentó el decreto 81 que regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado. Esta ordenanza tiene relación con el uso de firmas y de documentos digitales al interior de la Administración del Estado. El 9 de agosto de 2000 inició, como complemento, un proyecto de ley que regula la firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento voluntario de acreditación de prestadores de servicios de certificación, para su uso en actos o contratos celebrados por medio de documentos electrónicos a través de medios electrónicos de comunicación.¹⁹⁹

¹⁹⁶ Cfr. Reyes Krafft, Alfredo Alejandro, ob. cit, p.p. 110.

¹⁹⁷ Cfr. Ibidem, p.p. 131.

¹⁹⁸ Cfr. Ibidem, p.p. 132.

¹⁹⁹ Cfr. Ibidem, p.p. 152.

Ecuador.

En marzo de 2001, se presentó un Proyecto de Ley de Comercio Electrónico y firmas digitales, en términos similares a la chilena.²⁰⁰

Panamá.

En 31 de julio de 2001 se expide la Ley número 43, la cual define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico y el intercambio de documentos electrónicos.²⁰¹

Perú.

El 9 de agosto de 1999, se presentó el proyecto de ley que regula la contratación electrónica, el cual, fue dado a conocer en Washington DC en el seminario denominado “Responding to the Legal Obstacles to Electronic Commerce in Latin America”, organizado por National Law Center Inter American Free Trade. The organization of America States Business Software Alliance, tiene por objeto regular la utilización de la firma electrónica, otorgándole plena validez y eficacia jurídica equiparada al uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Se fundamenta en la legislación colombiana, argentina, chilena y mexicana, y fue aprobada por unanimidad por la Comisión de Reforma de Códigos.²⁰²

Venezuela.

El 26 de abril de 2000 se presentó un proyecto de Ley Orgánica de Tecnologías de Información, la cual tiene por objeto promover y desarrollar el uso intensivo de las tecnologías de información en la sociedad, y regular el régimen jurídico de la función y el servicio público del sector de tecnologías de información

²⁰⁰ Cfr. *Ibidem*, p.p. 153.

²⁰¹ Cfr. *Ídem*, p.p. 153.

²⁰² Cfr. *Ibidem*, p.p. 154.

estableciendo los principios orientadores y regulando los procesos de formación de políticas, normas, estrategias, planes y acciones tecnológicas de Estado a objeto de establecer la Infraestructura Nacional de Tecnologías de Información, entendida ésta como el conjunto de servicios y productos del sector de tecnologías de información, incluyendo aquellos que soportan el intercambio y difusión de información en dicha Nación a través de redes de transmisión de datos de carácter público o privado, pero de uso público, que se encuentren conectadas entre sí y a su vez que puedan conectarse con entidades similares en el exterior. Establece lineamientos e instituciones para regular el uso de la firma digital y los documentos electrónicos en la Administración del Estado; pero no considera al comercio electrónico.²⁰³

España.

La Circular del Banco de España 8/88 de 14 de junio, creó el reglamento del Sistema Nacional de compensación electrónica, que marcó un comienzo para la protección y seguridad necesaria para la identificación para el acceso a la información.²⁰⁴

El artículo 45 de la Ley 30/1992 de régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, incorporó el empleo y aplicación de los medios electrónicos en la actuación administrativa. Para su regulación el Real Decreto 263/1996, de 16 de febrero, indica que deberán adoptarse las medidas técnicas que garanticen la identificación y la autenticidad de la voluntad declarada, pero no hace ninguna regulación de la firma electrónica, sino hasta 1998, cuando en un Real Decreto del 17 de septiembre, se reconoce el uso de la firma electrónica, su eficacia jurídica y la prestación al público de servicios de certificación, y el 21 de octubre se convalida la Ley sobre Firma Digital con los votos a favor de PP (impulsor de proyecto) CIU, PNV y Coalición Canaria, y la oposición de PSOE y Grupo Mixto que no veían la urgencia de esta norma ni la necesidad de aprobarla como Real Decreto Ley.²⁰⁵

²⁰³ Cfr. *Ibidem*, p.p. 155.

²⁰⁴ *Ídem*.

²⁰⁵ Reyes Krafft, Alfredo Alejandro, *ob. cit.*, p.p. 156.

El 26 de octubre de 1998, luego de una serie difícil de negociaciones sobre los niveles de seguridad, el Parlamento Europeo aprobó una ley comunitaria que establece un marco común para la firma electrónica, y los ministros de la Comisión del Mercado de las Telecomunicaciones), son los encargados de velar por ello.²⁰⁶

Actualmente, se aprobó la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (ley 34/2002, de 11 de julio, publicada en el BOE el 12 de julio de 2002), que regula ciertos aspectos jurídicos de los servicios de la sociedad de la información y de la contratación por vía electrónica.²⁰⁷

Italia.

La ley de 15 de marzo de 1997 número 59, es la primera norma del ordenamiento jurídico italiano que recoge el principio de la plena validez de los documentos informáticos.

Asimismo, existen otras naciones como Francia, los países bajos (Dinamarca, Suiza y Bélgica), y el Reino Unido, que han estudiado de igual manera sobre la firma electrónica, y preparado sus legislaciones al cambio que impera a nivel mundial que representa la tecnología.

²⁰⁶ Ídem.

²⁰⁷ Reyes Krafft, Alfredo Alejandro, *La Firma Electrónica y las Entidades de Certificación*, editorial Porrúa, Sociedad Anónima de Capital Variable, Segunda edición, México 2008, p.p. 157.

Capítulo Tercero

El cheque electrónico

1. Concepto. ¿Forma especial del cheque o un nuevo cheque?

En sentido estricto, el cheque electrónico es un mensaje de datos que contiene la orden incondicional de pagar a la vista una suma determinada de dinero, emitido al destinatario, a cargo de una institución de crédito.

En sentido amplio, el cheque electrónico es una forma de pago consistente en

un mensaje de datos enviado por el emisor al correo electrónico del destinatario (acreedor), quien a su vez envía el documento electrónico con su firma electrónica avanzada al intermediario (institución bancaria), para que éste previa verificación de la identidad de aquel, libre los fondos a su cuenta bancaria.

La meta actual es que sea únicamente utilizado el cheque electrónico como un nuevo cheque; ello, derivado del avance tecnológico y la fiabilidad que éste empieza a consolidar.

Considero que de manera total sea utilizado el cheque electrónico como una nueva forma de pago, dado el alcance de la tecnología en todas las actividades, fruto de la renovación de nuestra mente; por lo que, no cabe utilizar las dos formas del cheque, esto es, el cheque sobre papel y el cheque electrónico; “Nadie pone remiendo de paño nuevo en vestido viejo”.

El mensaje que se revela es “ser frío o caliente”; los tibios son escupidos. Legislar el cheque electrónico, como una simple forma especial del cheque, sería como pintar la casa únicamente del frente, dejando los lados y la parte de atrás sin pintar. Por ello, se propone el desplazamiento total del cheque sobre papel, por un nuevo cheque, que en la actualidad lo representa el cheque electrónico.

Es importante destacar que motivado por el avance tecnológico, y las medidas de seguridad que ha originado certeza en las actividades comerciales por Internet, es loable que es el tiempo y el turno de nuestro país que forme parte de ese cambio en el mundo, y así, poder avanzar hacia nuevos retos, bien considerados como oportunidades.

Creo que nuestra nación tiene el potencial para encontrarse en el nivel económico competitivo mundial, y sea tierra deseable para que las empresas extranjeras tengan la certeza de invertir en nuestro país, y ello pueda crear oportunidades para todos; lo que en conjunto, genera crecimiento y desarrollo; en conclusión, una nueva nación.

De ello, se desprende la necesidad de actualizar los métodos y sistemas, y romper con los moldes que había dejado a nuestro país en rezago. Hoy competimos con naciones que han abierto sus ojos a las oportunidades que representa la tecnología. Mirar hacia atrás, representaría un detrimento para el propio desarrollo nacional.

Bajo esa tesitura, el cheque electrónico como forma de pago, puede generar mejores condiciones de seguridad y certeza para el cumplimiento de pago; mayor fluidez monetaria; menor costo de papel, lo que atrae aparejado el cuidado del medio ambiente; apertura económica; competitividad; multiplicación en la economía; en conclusión: desarrollo económico.

2. Naturaleza y elementos.

Por cuanto hace a la naturaleza del cheque electrónico, primeramente cabe establecer cuál es la naturaleza del cheque sobre papel, para así tener una mejor comprensión del porque se considera que el cheque electrónico es meramente un instrumento de pago. La palabra cheque, según la opinión más generalizada, es de “origen inglés”.²⁰⁸

Si bien, el cheque sobre papel, *formalmente*, es un título de crédito, considero que, esencialmente, es una forma de pago.

Como lo afirma el autor Arturo Díaz Bravo, el cheque es un documento más apropiado para el pago que para el crédito;²⁰⁹ asimismo, el escritor Felipe de J. Tena, refiere que el libramiento de un cheque no tiene más finalidad que el pago, finalidad que en sí misma, es del todo ajena a la idea de circulación, por lo que, al expedirse el cheque precisamente a la vista, el no poder presentarse sino en un plazo de breve duración, el no poder librarse sino contra una institución de crédito y siempre que en

²⁰⁸ De Pina Vara, Rafael, *Teoría y Práctica del Cheque*, editorial Porrúa, Sociedad Anónima de Capital Variable, Tercera edición, México, 1984, pág. 13.

²⁰⁹ Díaz Bravo, Arturo, *Títulos y Operaciones de Crédito*, IURE editores, Sociedad Anónima de Capital Variable Segunda edición, México 2006, p.p. 133.

ésta tenga depositados el librador fondos de que pueda disponer mediante cheques, son exigencias que únicamente se explican, por ser el título mero instrumento de pago; lo que demuestra esta naturaleza, concluye dicho autor.²¹⁰

En esa tesitura, comparto lo que afirma el autor José Gómez Gordoa, en el sentido de que debe ser sustituida la denominación de título de crédito (adoptado en nuestro país por la legislación italiana), por la de **título valor**, conforme a la doctrina alemana que utiliza esta denominación mediante las palabras germánicas *Wert Papier*, con la idea de que el título valor implica la unión del documento con el valor que representa;²¹¹ ello, en virtud de que cheque es un documento que tiene un derecho y correlativamente una obligación. Quien tiene el derecho es acreedor de una cosa, o a una suma de dinero que es un valor; por lo que, se adecua el término título valor, y no título de crédito como ha sido llamado el cheque por costumbre.²¹² Ejemplo notable, es la Ley de Concursos Mercantiles, la cual en sus artículos 10 y 20, utiliza el término “títulos valores”.

Asimismo, el autor Joaquín Rodríguez Rodríguez, señala que el cheque “es un instrumento de pago”²¹³, al manifestar que “Quien da un cheque lo hace como si diera dinero; quien toma un cheque, lo recibe como si obtuviese el pago en moneda de curso legal.”²¹⁴ De igual manera, el autor Enrique Sariñana Olavarría, manifiesta que el cheque “es un instrumento o medio de pago que sustituye económicamente el pago en dinero (monedas metálicas o billetes de banco)”.²¹⁵

Por su parte, existen criterios jurisprudenciales que señalan que la naturaleza del cheque es de instrumento de pago o forma de extinción de obligaciones; sin embargo, concluyen que el cheque al no ser cubierto por no existir fondos disponibles para ello, debe considerarse que contiene un derecho de crédito, ya que otorga al

²¹⁰ Tena, Felipe de J., *Derecho Mercantil Mexicano*, editorial Porrúa, Sociedad Anónima de Capital Variable, Vigésimo Primera edición, México 2006, p.p. 549.

²¹¹ Gómez Gordoa, José, *Títulos de Crédito*, editorial Porrúa, Sociedad Anónima de Capital Variable, Décima edición, México, 2007, p.p. 5.

²¹² Ídem

²¹³ Rodríguez Rodríguez, Joaquín, *Curso de Derecho Mercantil*, editorial Porrúa, Sociedad Anónima de Capital Variable, Vigésimo Cuarta edición, México 1999, pág. 366.

²¹⁴ *Ibidem*, p.p. 366 y 367.

²¹⁵ Sariñana, Enrique, *Derecho Mercantil*, editorial Trillas, Sociedad Anónima de Capital Variable, Primera edición, México 1999, pág. 28.

beneficiario del documento un derecho personal que por su propia naturaleza implica el cumplimiento de obligaciones de carácter pecuniario que mediante el ejercicio de las acciones jurisdiccionales respectivas, puede exigir del librador del documento; situación que no comparto como conclusión, en virtud de que existe contradicción en cuanto a que es distinta la naturaleza de un instrumento de pago con la de un crédito.

En sentido genérico, crédito (del latín *credere*), significa confianza. En sentido jurídico, habrá un negocio de crédito cuando el sujeto activo, que recibe la designación de acreditante, traslade al sujeto pasivo, que se llama acreditado, un valor económico actual, con la obligación del acreditado de devolver tal valor o su equivalente en dinero, en el plazo convenido.²¹⁶

El autor Pedro Astudillo Ursúa señala, “que hay un acto de crédito cuando en el intercambio falta la simultaneidad entre las prestación y la contraprestación de bienes, dinero o servicios; y a una prestación económica presente corresponde el compromiso de una contraprestación económica futura.”²¹⁷

El crédito existe cuando hay la entrega de una cosa presente por otra futura; esto es, se recibe una cosa presente por un pago futuro; un ejemplo, comprar a crédito una casa, en el que, se entrega el inmueble, y el precio se paga luego de cierto plazo.

Nace de la imaginación de los comerciantes de cómo aumentar sus ventas y evitar los riesgos de robo de sus mercancías, aunado a que la premisa en el comercio es que los ingresos no coinciden, en tiempo, con las necesidades, fue así como el comerciante arriesgó y se introdujo en esta nueva etapa del comercio.²¹⁸

El autor Arwed Koch, entiende por crédito “la disposición, desde el punto de vista del acreditante, y la posibilidad, desde el punto de vista del acreditado, de efectuar un contrato de crédito, esto es, un contrato cuya finalidad es la producción de

²¹⁶ Cervantes Ahumada, Raúl, *Títulos y Operaciones de Crédito*, editorial Porrúa Sociedad Anónima de Capital Variable, Décima Séptima edición, México, 2007, p.p. 208.

²¹⁷ Astudillo Ursúa, Pedro, *Los Títulos de Crédito*, editorial Porrúa, Sociedad Anónima de Capital Variable, Séptima edición, México 2006, pág. 5.

²¹⁸ Dávalos Mejía, Carlos Felipe L., *Títulos y Operaciones de Crédito*, Oxford University Press México, Sociedad Anónima de Capital Variable, Tercera edición, México 2002, p.p. 9 y 10.

una operación de crédito”.²¹⁹ Entre algunos ejemplos de contrato u operaciones de crédito, se encuentran: el reporto, la apertura de crédito, el contrato de carta de crédito, y los contratos refaccionarios y de habilitación o avío.

Por su parte, el autor Víctor M. Castrillón y Luna, describe al crédito como la tercera etapa de la actividad comercial que “facilita el postergamiento de las operaciones comerciales, para ser cumplidas en tiempo posterior o en forma sucesiva”.²²⁰

En esa tesitura, se puede citar como principales diferencias entre el cheque y el crédito en su forma más simple, las siguientes:



Es clara la diferencia total que existe entre la naturaleza del cheque y del crédito. El cheque es una forma de pago, en la que si bien nace a la vida jurídica, de un contrato de depósito a la vista (considerado *formalmente* como una operación de crédito), el cheque funciona meramente como un instrumento de extinción de una obligación de pago.

²¹⁹ Ídem.

²²⁰ Castrillón y Luna, Víctor M., *Titulos Mercantiles*, editorial Porrúa, Sociedad Anónima de Capital Variable, Segunda edición, México, 2008, p.p. 4.

El depósito bancario a la vista es formalmente una operación de crédito; no obstante, considero que, en estricto sentido, no tiene la naturaleza de un crédito; pues, dicho depósito no se hace bajo una promesa, sino bajo un mandato de pago (término “mandato” utilizado en sentido genérico); por consiguiente, si bien el banco recibe riqueza al momento en que le es transmitida la propiedad del numerario, materialmente lo que existe es un resguardo de dinero que el librado está obligado a custodiar para efecto de estar en aptitud de pagar los cheques que emita el depositante a su cargo.

Por su parte, se ha buscado equiparar la “orden incondicional de pago” del cheque, con la “promesa de pago a futuro” en el crédito; situaciones que son distintas; toda vez que en el cheque no es necesario el elemento confianza, pues el que recibe un cheque lo hace como si obtuviera el pago en moneda de curso legal.

Tampoco, pueden equipararse las partes que intervienen en el cheque con las que interviene en el crédito.

El librador no puede equipararse a un acreditado, toda vez que aquél extingue una obligación a través de una orden incondicional de pago a la vista; el acreditado, por su parte, se encuentra constreñido a pagar en un plazo determinado para extinguir su obligación de pago, determinado por un contrato.

Por otra parte, el beneficiario no puede hacer las veces de un acreditado, toda vez que aquél no recibe riqueza, sino un pago. De la misma forma, no se puede equiparar el beneficiario con el acreditante, en virtud de que éste se desprende de una cosa y el beneficiario recibe un pago.

De todo lo anterior se advierte, que la naturaleza del cheque es ajena a la del otorgamiento de un crédito; por ende, no se le puede dar la terminología de “título de crédito”; sino, de “título valor con fines de instrumento de pago”.

En ese sentido, se propone el cheque electrónico, el cual, a diferencia de la

naturaleza formal del cheque sobre papel, aquél es eminentemente un instrumento de pago, cuyas características son las de un cheque certificado para abono en cuenta; por lo que, ha de ser nominativo, no negociable y, por ende, no endosable. Solamente el destinatario tiene la facultad de presentarlo al cobro dentro del plazo de veinticuatro horas a la institución intermediaria, quedando ésta obligada a pagarlo con las responsabilidades de un principal obligado. Esto es, “la persona a favor de la cual se expide el cheque tiene la titularidad del documento, y tiene la idoneidad para ejercitar los derechos que el mismo consigna.”²²¹

Es así como el banco intermediario se obliga cambiariamente frente al destinatario a pagarle ese cheque, generándose así una relación jurídica obligacional entre aquel y el destinatario. Las acciones contra la institución intermediaria en este supuesto, prescriben en seis meses, contados a partir de la fecha en que concluya dicho plazo de presentación.

Dicha obligación cambiaria nace mediante la firma electrónica avanzada del documento, pues quien firma, “crea una cosa mercantil”.²²²

Asimismo, el cheque electrónico, es un título de circulación o “títulos circulatorios”²²³, aún si bien su naturaleza de medio de pago, pues ya desde que se emite a favor de persona alguna, ya es un documento que circula; por lo que, no puede equiparse al cheque con boletos, contraseñas, fichas u otros documentos que no están destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consigna.

Por ende, no estoy de acuerdo, en lo que interesa, con lo que afirman los autores Felipe de J. Tena y Navarrini, al expresar respectivamente, que el cheque “no tiene más finalidad que el pago, finalidad que en sí misma, es del todo ajena a la idea de circulación”;²²⁴ y, que el cheque “es simplemente una orden de pago, un título de

²²¹ Becerra Bautista, José, *El Cheque sin Fondos*, editorial Kino, Sociedad Anónima, Cuarta edición, Tijuana, B.C. 1973, pág. 155.

²²² Mantilla Molina, Roberto L., *Titulos de Crédito*, editorial Porrúa, Sociedad Anónima de Capital Variable, Segunda edición, México, 1983, pág. 35.

²²³ Escuti, Ignacio A., *Titulos de Crédito*, Tercera edición, Editorial Astrea de Alfredo y Ricardo Desalma, Buenos Aires 1992.

²²⁴ Gil y S, José Pérez, *El cheque sin fondos*, Imprenta “Zavala” San Ildefonso y Carmen, México 1945, pág. 23.

exacción, un título que sirve para liquidaciones y pagos, no un título de circulación”.²²⁵

El cheque electrónico es una forma de asegurar el pago, pues una cualidad de este documento electrónico, como ya se ha dicho con antelación, es la de un cheque certificado; en tal virtud, siempre será pagada la suma determinada en el mismo, dado que el emisor previo al envío del cheque electrónico al correo electrónico del intermediario, debe solicitar a la institución bancaria la certificación del mismo; es así como el banco intermediario realiza un cargo contable en la cuenta de depósito bancario de dinero que lleva, a partir de ese momento le disminuye su saldo con el importe precisamente de ese cheque, automáticamente abre una cuenta deudora a cargo de la propia institución y a favor del destinatario del cheque y queda a la espera de que éste envíe el cheque para pagárselo. En esas condiciones, el emisor no está autorizado para emitir un cheque electrónico, sin que previamente haya sido certificado por el banco intermediario.

Como elementos del cheque electrónico se encuentran: a) el emisor o deudor; b) el intermediario (institución de crédito-banco); y, c) destinatario o acreedor.

a) Emisor o deudor. Es la persona que teniendo fondos en una institución de crédito, sea autorizado por ésta para emitir cheques electrónicos a su cargo. En términos amplios, el emisor es la persona que envía o genera el cheque electrónico o mensaje de datos; ello, con el ánimo de extinguir una obligación de pago.

b) Destinatario o acreedor. Es la persona en favor de quien se emite el cheque electrónico; esto es, es la persona que recibe en su cuenta de correo el cheque electrónico para que esté en aptitud de renviarlo a la institución de crédito, y pueda ser cobrado. Al destinatario también se le puede llamar “beneficiario”; sin embargo, este término da la idea de cualquier persona que con el pago que recibe encuentra un beneficio, y no específicamente un pago; por ello, el nombre de “acreedor”, es un término que apunta netamente hacia una persona que tiene un derecho a pedir el

²²⁵ Ibidem, pág. 24.

cumplimiento de una obligación, en el presente caso, de pago; obligación que es extinguida al momento en que el destinatario recibe en su cuenta de correo el cheque electrónico.

c). Intermediario. Es la institución de crédito que actuando por cuenta de otro (emisor), tiene la obligación de librar los fondos a la cuenta bancaria del destinatario, previa recepción del cheque electrónico y verificación de la firma electrónica avanzada de éste. Es el banco, quien en función del servicio financiero que presta, libra los fondos iguales a la orden incondicional de pago que se emite.

Por otra parte, los requisitos formales del cheque electrónico son: i). la mención de ser cheque, inserta en el texto del documento; ii). el lugar, la fecha y la hora en que se emite; iii). la orden incondicional de pagar una suma determinada de dinero; iv). el nombre del intermediario; v) el nombre del destinatario; vi). el lugar de pago (la orden de pago puede ser para el propio banco intermediario o para depósito en otro banco), y vii). la firma electrónica avanzada del emisor; viii). la cuenta bancaria del destinatario; y, en caso de que el cheque contenga la orden de depositarlo en otro banco, se indicará ix). el nombre del banco receptor, y x) la cuenta CLABE o cuenta bancaria estandarizada del destinatario.

En términos de seguridad, el cheque electrónico cuenta con la firma electrónica avanzada, la criptografía, y las claves pública y privada; lo que imposibilita el robo de cheques, y minimiza los conflictos, que en la actualidad se ventilan ante los Tribunales, derivados del cobro de cheques mediante firmas falsificadas, y en donde el titular se ve obligado a recurrir a instancias como la CONDUSEF, a efecto de convenir con la institución bancaria para que ésta rembolsa el dinero sustraído; situación que difícilmente acontece.

Es así como se concluye, que el cheque electrónico responde al marco actual tecnológico, que en mucho rebasa al cheque sobre papel en términos de confiabilidad, transparencia, seguridad y certeza.

3. Presupuestos.

Como presupuestos del cheque electrónico se tienen los siguientes:

a). Es un título valor con fines de instrumento de pago; por tanto, no producirá efectos de título de crédito.

b). Técnicamente, es un mensaje de datos enviado por el emisor al correo electrónico del destinatario, quien a su vez renvía el documento electrónico con su firma electrónica avanzada a la institución bancaria intermediaria, para que ésta previa verificación de su identidad, libre los fondos a la cuenta bancaria del destinatario.

c). El cheque electrónico tiene las características de un cheque certificado para abono en cuenta; por lo que, ha de ser nominativo, no negociable y, por ende, no endosable. El pago se perfecciona en el momento en que es recibido el cheque electrónico en la cuenta de correo electrónico del destinatario.

d). El cheque electrónico será siempre pagadero al momento de que el intermediario reciba documento electrónico a la cuenta de su correo electrónico.

e). El pago de un cheque electrónico deberá ser siempre en su totalidad.

f). Sólo puede ser emitido por quien teniendo fondos disponibles en una institución de crédito, esté autorizado para emitir cheques electrónicos a su cargo a través de la utilización de una chequera electrónica. Dicha autorización se entenderá conferida al emisor que previamente a la emisión del cheque electrónico, haya solicitado a la institución bancaria intermediaria su certificación.

g). El emisor deberá enviar el documento encriptado con la llave pública del destinatario, quien deberá descifrarlo con su llave privada. El emisor y el destinatario deberán acordar sobre el acuse de recibo del mensaje de datos, por lo que

el destinatario está obligado a acusar recibo en la forma determinada con el emisor.

h). El destinatario luego de recibido el cheque electrónico en su cuenta de correo, deberá reenviar dicho documento electrónico encriptado con su firma electrónica avanzada a la institución bancaria intermediaria para su pago. El intermediario luego de verificar las firmas electrónicas avanzadas del emisor y destinatario, deberá librar los fondos que respalde el cheque electrónico a la cuenta bancaria de éste.

i). El destinatario tiene el plazo de veinticuatro horas, a partir de que éste reciba el cheque electrónico en su cuenta de correo electrónico, para el cobro de dicho documento. En caso contrario, deberá reenviar el cheque electrónico no cobrado nuevamente al emisor quien lo archivara conforme al sistema establecido, para su ulterior consulta.

j). El emisor, en caso de no ser presentado el cheque electrónico en el plazo indicado, podrá revocar el cheque, oponerse a su pago, y disponer de dichos fondos para la emisión de otro cheque electrónico.

k). Cuando, sin justa causa, se niegue el intermediario a pagar un cheque electrónico, resarcirá al destinatario los daños y perjuicios que con ello le ocasione. En ningún caso la indemnización será menor del veinte por ciento del valor del cheque. Las acciones contra la institución intermediaria en éste supuesto, prescriben en seis meses, contados a partir de la fecha en que concluya el plazo de presentación.

l). El pago del emisor al destinatario se acredita con el documento electrónico que en vía de notificación emite el banco intermediario.

m). La muerte o la incapacidad superveniente del emisor, no autorizan al intermediario para dejar de pagar el cheque electrónico.

n) La declaración de que el emisor se encuentra en estado de concurso, no obliga al intermediario, desde que tenga noticia de ella, a rehusar el pago.

4. Diferencias entre cheque electrónico y transferencia electrónica.

La diferencia esencial se encuentra en que el cheque electrónico, tiene la finalidad de pago y extinguir una obligación. La transferencia electrónica, puede bien utilizarse como un medio de pago, o para otro fin, como lo sería una simple transferencia a mi hijo para que esté en aptitud de comprar material escolar.

A través del pago mediante cheque electrónico, garantizo el cumplimiento de pago y, por ende, la extinción de una deuda preexistente; pues como se ha mencionado con antelación, el pago se perfecciona en el momento en que es recibido el cheque electrónico en el correo electrónico del destinatario.

Actualmente, en México existe un sistema de pago mediante transferencia entre cuentas bancarias, llamado *sistema de pagos electrónicos interbancarios* (SPEI), que empezó a operar el 13 de agosto de 2004, y que fue desarrollado por el Banco de México, el banco central de la Nación, y la banca comercial, para permitir a los clientes de los bancos enviar y recibir transferencias electrónicas de dinero en minutos.²²⁶

El SPEI, permite realizar transferencias de fondos entre sus participantes. La persona física o moral puede solicitar este servicio directamente al banco donde tiene su cuenta. Las transferencias se instruyen desde una cuenta bancaria, a través del servicio de banca por Internet; por lo que, se debe registrar la cuenta beneficiaria del pago, e ingresar a la sección de transferencias o pago a terceros y proporcionar los datos de la transferencia (cuenta beneficiaria, banco del beneficiario y monto). Los participantes pueden asignar prioridad alta a algunos pagos y reservar parte de su saldo para liquidar exclusivamente estos pagos. Cuando el sistema recibe una instrucción de pago, la almacena en una cola de pagos pendientes. Esto es, si un pago

²²⁶ banxico.com

no puede realizarse por falta de liquidez del participante que lo envía, éste permanece en la cola de pagos pendientes. Los bancos participantes envían los pagos que soliciten sus cuentahabientes a más tardar diez minutos después de aceptar la solicitud; asimismo, los bancos receptores de un pago deberán acreditar la cuenta de su cliente beneficiario a más tardar 10 minutos después de recibir el aviso de que se ha liquidado el pago. La seguridad del SPEI está basada en mensajes firmados digitalmente, así como el uso de certificados digitales, y el uso de claves de las personas autorizadas.

Ahora bien, cuál es la diferencia entre el sistema de pago interbancarios (SPEI), y el cheque electrónico que se propone. ¿Cuáles son las desventajas que representa aquél sistema de pago interbancarios, en comparación con las ventajas que representa el cheque electrónico?.

SPEI únicamente tiene cobertura dentro del territorio nacional, mientras el cheque electrónico tiene cobertura a nivel mundial. Mientras SPEI actúa como transferencia electrónica y/o medio de pago; el cheque electrónico actúa netamente como forma de pago. En el sistema SPEI existe un rubro en donde el cliente debe asentar el concepto de la transferencia, es decir, si es una simple transferencia, o un pago; dichos rubros no son obligatorios para el cliente, quien si no advierte tal omisión, puede enviar la transferencia sin concepto; lo que puede generar confusión para el beneficiario al momento de recibir el depósito si éste no tiene conocimiento de dicha transferencia. En consecuencia, el ordenante se encuentra en desventaja para acreditar el pago en este sistema, si aquel es objetado, ya que si el emisor no asentó el motivo o concepto de la transferencia, no existe certeza de que realmente la transferencia se hizo con el ánimo de cumplir con una obligación de pago.

En el cheque electrónico, el beneficiario tiene la certeza de que el envío de dicho documento electrónico es indicativo de que el emisor cumple con una obligación de pago.

Por otra parte, el cheque electrónico es un mensaje de datos dotado de mayor

seguridad en cuanto al proceso de generación, envío, recibo o archivo; ello, en virtud de que éste utiliza la firma electrónica avanzada; a diferencia de SPEI, el cual, únicamente utiliza una firma electrónica.

Recibido el cheque electrónico en el correo electrónico del acreedor, éste tiene garantizado el pago; ello, en virtud de la provisión garantizada que existe en el banco intermediario. Lo contrario a SPEI, toda vez que en este sistema de pago, el cliente puede solicitar una transferencia, no obstante, no cuente con una provisión que respalde dicha solicitud; en este caso, el banco puede retener estos pagos y ponerlos en lo que se llama “una cola de pagos”. Esto es, en SPEI se da por cumplida la obligación desde el momento en que se encuentra la transferencia en la cuenta del beneficiario; lo que no sucede con el cheque electrónico, pues en esta forma de pago, la obligación se tiene por cumplida al momento en que aparece el cheque electrónico en la cuenta de correo del beneficiario.

En el sistema SPEI las solicitudes de transferencia únicamente se pueden hacer en las horas de oficinas del banco, esto es, hasta las 17:30 horas, o bien, en Internet de las 6:00 a las 17:30 horas. El cheque electrónico en cualquier momento puede ser enviado, y cobrado ante la institución de crédito a través de Internet.

Por otro lado, la relación dentro del SPEI únicamente se da entre el cliente y el banco emisor, en donde el beneficiario puede tener o no conocimiento al momento de la transferencia. En el cheque electrónico las partes tienen conocimiento directo en todo el proceso de pago. Un ejemplo concreto, en la utilización de SPEI y cheque electrónico, es el siguiente:

Ejemplo. Pago mediante SPEI.

- Juan debe depositar la colegiatura de su hijo cada 2 de cada mes. Por lo que Juan contrató el servicio SPEI, para que cada dos de cada mes, la institución bancaria en donde se encuentra aperturada su cuenta, transfiera la cantidad respectiva por concepto de pago de colegiatura de su hijo al Colegio donde se encuentra estudiando.

Aquí el colegio espera en su cuenta bancaria la cual está registrada mediante su CLABE ante la institución bancaria, que cada día 2 de cada mes encuentre el depósito del hijo de Juan por tal concepto. Sin embargo, ese día 2, hubo una complicación con la red, y no hubo posibilidad de hacer transferencias. Por lo que hasta el día siguiente fue depositada la colegiatura. Aquí ya hubo un retraso de pago, y responsabilidad para Juan.

Ejemplo. Pago mediante cheque electrónico.

- Juan tiene aperturada una cuenta de cheques electrónicos, y cada día 2 de cada mes, él envía un cheque electrónico a la cuenta electrónica del Colegio donde asiste su hijo; recibido éste el mismo día, el Colegio cuenta con 24 horas para realizar el cobro del mismo ante la institución bancaria respectiva. Desde el momento en que es recibido el cheque, se tiene por cumplido el pago de la colegiatura. Juan ya no tiene que preocuparse si ese día lo cobra el Colegio o al día siguiente, o si hubo una complicación con la red. El Colegio envía el cheque electrónico a la institución bancaria el mismo día para su cobro, y ese mismo día hubo problemas con la red. Sin embargo, aquí Juan ya no tiene responsabilidad, pues el pago se encuentra perfeccionado desde el día 2, momento en que el cheque fue recibido en la cuenta electrónica del Colegio.

En conclusión, el cheque electrónico representa por antonomasia, una forma eficaz de pago actual, que en mucho rebasa al SPEI, como formas de pagos interbancarios.

5. Forma de uso del cheque electrónico en México.

Actualmente, el banco BANORTE utiliza la forma llamada *check*; sin embargo, no es propiamente un cheque electrónico, sino una simple transferencia entre cuentas bancarias entre empresas.

Es un servicio, el cual le permite recibir pagos por Internet con cuentas

Banorte (cuentas de cheques, débito y crédito), recibiendo los recursos de las transacciones en línea a una cuenta de cheques. Los beneficios que se cuentan con este producto, son que permite aceptar las operaciones con cheques Banorte; garantiza el depósito de los fondos; y, los pagos son recibidos en línea.²²⁷

Como requisitos para la obtención de este servicio, se encuentran:²²⁸

- i). Tener una cuenta de cheques tradicional Banorte.
- ii). Firmar un contrato y anexar la documentación requerida.
- iii). Entregar a sus clientes las fichas de pago para recepción en sucursal.

Del esquema anterior, se desprende que no es propiamente un cheque electrónico el que se expone, sino más bien, un servicio a través del cual las empresas pueden realizar transferencias electrónicas entre sí. De lo que se advierte, que aún no se encuentra en la práctica, el cheque electrónico como forma de pago en México.

6. Funcionamiento, práctica y utilidad actual del cheque electrónico como medio de pago en Estados Unidos de América.

En octubre de 2003 el congreso de los Estados Unidos, aprobó la ley Check 21 o “Check Clearing for the 21st Century Act” (en español “Intercambio de cheques en el siglo 21”). Entró en vigencia el 28 de octubre de 2004, y afecta a todas las instituciones financieras de Estados Unidos. Su objetivo es reducir el papeleo, combatir el fraude y agilizar la forma en que el sistema bancario procesa los cheques.²²⁹ La ley Check 21 reemplaza a cualquier ley federal o estatal, incluidas las disposiciones del Uniform Commercial Code (Código Comercial Uniforme); en la medida en que tales leyes sean incompatibles con esta ley. Las leyes que se aplican a los cheques y que no sean incompatibles con la ley Check 21 se siguen aplicando.²³⁰

²²⁷ www.banorte.com

²²⁸ Ídem.

²²⁹ www.wachovia.com

²³⁰ Ídem.

Los principales objetivos de la ley Check 21 son:²³¹

- Alentar a los bancos para que usen la presentación digitalizada de los cheques, permitiendo que un cheque sustituto reemplace al cheque original.
- Fomentar la innovación en el sistema de cobro de cheques.
- Mejorar la eficiencia general del sistema de pagos de Estados Unidos.
- Reducir el tiempo que tardan los cheques en compensarse, dependiendo más de la automatización y menos del procesamiento manual de cheques.

Actualmente, más de 40 mil millones de cheques son emitidos anualmente en los Estados Unidos y recorren un largo trayecto desde que son emitidos. Cuando es emitido un cheque, éste es canjeado por efectivo o depositado en una institución financiera, procesado por Cooperativa o por bancos, y luego enviado a su Cooperativa de Crédito para su cobro. Todo este trayecto de los cheques es costoso y representa miles de millones de dólares al año.²³²

Esta iniciativa ha traído como beneficios a las instituciones financieras como el ahorro en el costo de transportes de valores, menores costos de gestión y tiempo; eliminación de barreras geográficas, la generación de menor tiempo de procesamiento;²³³ lo que elimina las demoras para el envío de cheques y, por ende, los depósitos de cheques en la cuenta del cliente se compensan más rápidamente.²³⁴

Una mayor rapidez en el procesamiento de los cheques significa una menor flotación. La mayor rapidez en el cobro y en la devolución de los cheques reduce notoriamente los fraudes en el sistema de cobranzas de cheques; ello, a través del nuevo tipo de documento de pago denominado “cheque sustituto”, el cual, es una

²³¹ Ídem.

²³² www.nafcu.com

²³³ www.ebanking.cl

²³⁴ <http://español.regions.com>

reproducción en papel de un cheque original, creado durante el proceso de cobro y devolución del cheque a partir de una imagen electrónica del original.²³⁵

Un cheque sustituto es una imagen digital del cheque original.²³⁶ Contiene la misma información que un cheque original, y siempre incluye un texto que lo identifica como una copia legal del cheque original: “This is a legal copy of your check. You can use it the same way you would use the original check” (en español: “Ésta es una copia legal de su cheque. Puede usarlo de la misma forma en que usaría el cheque original”).²³⁷

Las instituciones financieras destruyen el cheque original poco después de efectuar la copia electrónica²³⁸, o lo que se llama “truncar”; esto es, cuando se emite un cheque, el banco que deposita el mismo puede elegir truncarlo. Truncar significa que el banco captura la imagen del cheque original, por ambos lados, y el original es destruido. La imagen del cheque, conjuntamente con la información codificada en la parte inferior de la imagen, es procesado por la cámara de compensación.²³⁹

El cheque sustituto es utilizado únicamente entre bancos; ello, con el propósito de agilizar el proceso de pago e intercambio de información de esta forma; en tal virtud, los cheques sustitutos no se aceptan como pago de productos o servicios; sino que éstos sólo se crean durante el proceso de cobro y devolución del cheque para reemplazar el original.²⁴⁰

Fuente: www.federalreserve.gov

Figura 13. Cheque sustituto.

²³⁵ www.nafcu.com

²³⁶ www.ebanking.cl

²³⁷ www.wachovia.com

²³⁸ www.federalreserve.gov

²³⁹ www.enbfl.com

²⁴⁰ Ídem



Frente de un cheque sustituto.



Dorso de un cheque sustituto.

Es decir, el banco captura el cheque original, y lo reproduce de manera electrónica, para luego utilizarlo éste, ya sea para su cobro o devolución. El cheque original se destruye, y sigue en circulación el cheque sustituto, el cual, en caso de presentarse en un diverso banco al librado, a aquel se facilita la transferencia electrónica de imágenes, en lugar del intercambio físico de cheques originales de papel para su cobro.²⁴¹

Actualmente, se reciben los cheques pagados junto con el estado de cuenta o si se solicitan fotocopias de cheques pagados, es posible que se reciba una combinación de cheques originales y sustitutos; ello, protegido por las leyes federales y estatales por errores cometidos en la cuenta aún si recibe los cheques pagados (originales, sustitutos o ambos) con su estado de cuenta, en un estado de cuenta con imágenes de cheques sustitutos, o en un estado de cuenta que simplemente describe los cheques

²⁴¹ www.federalreserve.gov

pagados.²⁴² En caso de que se reciba un cheque sustituto y un problema o error del mismo le ocasiona una pérdida monetaria, Check 21 dispone de un procedimiento especial, que únicamente aplica para éste tipo de cheques, que permite solicitar un reembolso (llamado "crédito restituido agilizado").²⁴³

7. Importancia y necesidad de implementar y regular el cheque electrónico como medio de pago en México.

En la medida en que México avance hacia el cambio que produce renovación, y fije su mirada hacia las oportunidades que ofrecen los nuevos adelantos tecnológicos, podrá participar en una economía actual, que lo integre con otras economías, que hoy son punta de lanza en la materia.

No es conveniente estancarse en moldes, ni en los temores que paralizan una nación. Si bien, todo cambio, al principio produce temor, no lo es cuando existe una promesa de avance, desarrollo y crecimiento.

Dejar el pasado y mirar hacia delante es lo que nuestro país necesita, menos quejas y más esfuerzo, menos crítica y más trabajo duro, menos incertidumbre y más certeza y oportunidades.

Existe actualmente una necesidad de adquirir conocimiento. Cada minuto el hombre crea algo. Somos por naturaleza creadores. Creamos e inventamos lo que primero se establece como una idea, y luego se concreta en lo físico. Aprovechar la creación y administrarla de manera eficaz, lleva a una nación a consolidar oportunidades que generen riqueza en conocimiento, que da por añadidura riqueza material.

En México existen hombres y mujeres con cualidades, virtudes y sueños que pueden ser utilizados. En México existen los recursos que pueden ser explotados.

²⁴² Ídem.

²⁴³ Ídem.

México, requiere personas con valor, que dejen las malas actitudes, y se esfuercen por lograr sus metas. México puede llegar a ser una potencia, en la medida que lo creamos. México es nuestra casa, limpiemos la casa y empecemos a renovarla.

El comercio electrónico en los países desarrollados representa más del 2% del producto interno bruto. En otros países como España, se ha creado la figura del Master, es decir, carreras en donde enseñan al alumno a diseñar negocios electrónicos.

Como estadística importante, actualmente se hace una venta cada segundo mediante el comercio electrónico. Eso equivale a 60 productos vendidos en un minuto; lo que equivale a 600 productos en una hora; 14,400 productos en un día; equivalente a 432 mil productos en un mes. En un año *5 millones 184 mil productos vendidos*.

Estas cifras son tomadas de las estadísticas que Mercado Libre hace actualmente, y que informa en relación a los productos que se venden a través de Internet.

Es visible que está pasando algo, un cambio radical en las formas de comerciar, no solo de bienes, sino también de servicios. Entre esos cambios, el cheque electrónico como forma de pago.

No es suficiente la intención de regular el cheque electrónico como una forma especial del cheque, sino como un nuevo cheque que desplace al cheque sobre papel. Si bien en México, se ha legislado sobre comercio electrónico, lo que representa un avance y un lugar importante en relación con otras naciones que también preocupadas y ocupadas por el tema han legislado al respecto, aún falta abordar el tema relativo al cheque electrónico como medio de extinción de obligaciones. Situación que creo no será difícil puesto que están sentadas las bases, en cuanto a la regulación de la firma electrónica avanzada, valor probatorio de los documentos electrónicos, mensajes de datos, etcétera.

Es necesario establecer instrumentos que tutelen penalmente el cheque electrónico. “Es indispensable dotar de seguridad y certeza jurídicas en su circulación y realización.”²⁴⁴

Dadas las características de esta forma de pago, esto es, en su naturaleza de cheque certificado, conviene señalar que a este medio de pago, no se adecua lo previsto en el artículo 386, fracción XXI, del Código Penal Federal; es decir, no se tipifica como un delito de fraude la conducta antijurídica en la que se utilice un cheque electrónico, sino, dicha conducta ilícita se encuadra dentro de un delito informático, regulado en el Título Noveno, Capítulo II, del Código Penal Federal, relativo al acceso ilícito a sistemas y equipos de informática.

Aún falta encuadrar cada conducta antijurídica que pueda suscitarse a este tipo penal, esto es, cada conducta ilícita que pueda derivarse del uso incorrecto del cheque electrónico, bajo el principio de *nullum crimen sine lege y nulla poena sine lege*; y así, poder imponerse penas que tengan una base legal, o bien, disposición alguna que castigue el acto por el cual se imponen, o que el acto que les da origen esté exactamente comprendido en las disposiciones legales que lo castiguen.

Ello, para efecto de que se le dé mayor seguridad, y se repriman los usos impropios que del mismo instrumento puedan hacerse. Llamada a influir la institución del cheque, tanto en la esfera pública del interés colectivo, como en la esfera negocial del tenedor del libramiento.²⁴⁵

Falta por alcanzar metas, y no únicamente en lo que respecta al cheque, sino en otros temas. La tecnología cambia continuamente, y hoy más, existe la necesidad de implantar el documento electrónico, en solidaridad con el apoyo al cuidado del medio ambiente.

²⁴⁴ Orizaba Monroy, Salvador, *El Cheque*, editorial SISTA, Sociedad Anónima de Capital Variable, Primera edición, México, 2005, pág. 9.

²⁴⁵ Cfr. Domínguez del Río, Alfredo, *La Tutela Penal del Cheque*, editorial Porrúa, Sociedad Anónima de Capital Variable, Primera edición, México, 1974, p.p. 164 y 165.

Se visualiza el tiempo en el cual todo o la gran parte de las relaciones comerciales, diplomáticas, jurisdiccionales, sean a través de los medios electrónicos; lo que impera una necesidad de impulsar iniciativas que fomenten y motiven la utilización de las nuevas tecnologías de información y comunicación; en el presente caso, la iniciativa sobre la regulación del cheque electrónico, que más allá de ser una simple forma de pago, es un medio seguro y confiable de extinguir una obligación contraída, sin necesidad del manejo de dinero en efectivo.

En ese sentido, es importante en México dotar al cheque de las cualidades que le han sido atribuidas al “cheque sustituto” en la práctica bancaria en Estados Unidos, y que no disiente con el cheque electrónico que se propone en el presente apartado.

Además de que el cheque electrónico, representa como beneficios, los siguientes:

1. Ahorro para los bancos.
2. Rompe las barreras del papel, que genera mayor fluidez monetaria.
3. No es susceptible de extravío y/o falsificarse la firma del librador.
 4. Existe la certeza de que el cheque se pague al momento de su emisión a la institución bancaria intermediaria.
 5. Conservación del medio ambiente en ahorro de papel.
 6. Inserción de México en el fenómeno globalizador; en especial, en la nueva modalidad de comercio llamada “comercio electrónico”.

Ahora bien, ¿porqué la necesidad “actual” de regular el cheque electrónico?

En atención a las estadísticas del INEGI, en México, aproximadamente el 55% de la población, es población económicamente activa (PEA), de los 14 años en adelante. Considerando que el cheque es utilizado por persona mayor de 18 años, dado que puede contar con una cuenta bancaria, y existen medios que lo identifican

(credencial para votar, pasaporte, cédula, etcétera); se excluyen a las personas que tengan entre 14 y menos de 18 años de edad. Esto representa un aproximado del 50% de la población total, que factiblemente ha utilizado el cheque; esto es, aproximadamente 50,000,000 de personas, que en algún momento han utilizado el cheque.

En México, el 30% de los hogares, cuenta con una computadora. Por lo que, se estima que una persona económicamente activa, habita en cada uno de esos hogares, resultando 30,000,000 de personas económicamente activas, aproximadamente, que cuentan con una computadora personal. Ello representa, el 60% de la PEA.

No obstante, esto no quiere decir que, el 40% del PEA restante, no tenga a su alcance una computadora; dado el surgimiento del servicio de Internet que actualmente ofrecen las bibliotecas públicas, así como los llamados “cibercafés”; y, considerando que en las comunidades indígenas (en las cuales se encuentra el 7% del PEA), aún no se encuentra la penetración de las tecnologías de información y comunicación; se concluye que, sólo este 7%, no podría de inmediato utilizar el cheque electrónico; lo que, representa un 12% del PEA, un 7% de la población total.

Por lo que, se llega a la conclusión, que es el turno de México, para aprovechar los beneficios que representan las tecnologías de información y comunicación y, en lo que respecta a la materia, aprovechar los beneficios que representa el cheque electrónico.

Cabe destacar, que la población indígena se encuentra, de igual forma, en una renovación del pensamiento. Actualmente, la estructura por edad muestra porcentajes mayores de menores de 15 años. Entre los miembros de menores de edades se concentran los mayores porcentajes de quienes no hablan lengua indígena; ello, motivado por la alfabetización en esas poblaciones, la cual, junto con la educación, han favorecido al aprendizaje en la ciencia. De tal forma que, no dudo que esta nueva generación busque integrarse al fenómeno globalizador, y aproveche la utilización de

las nuevas tecnologías de información y comunicación, en lo que favorezca para el bien común.

8. Propuesta de reforma al Código de Comercio y a la Ley General de Títulos y Operaciones de Crédito.

Se propone que el cheque electrónico sea regulado en la Ley General de Títulos y Operaciones de Crédito, en un apartado relativo a los “títulos valores”.

Por lo que, se propone la reforma al artículo **75, fracción XIX**, del Código de Comercio, para quedar como a continuación se establece:

“Artículo 75. La ley reputa actos de comercio:- - - XIX. Los cheques electrónicos, letras de cambio ó remesas de dinero de una plaza á otra, entre toda clase de personas.”

En ese sentido, se propone la reforma del artículo 1º, de la Ley General de Títulos y Operaciones de Crédito, para quedar como sigue:

“Artículo 1. Son cosas mercantiles los títulos de crédito y los títulos valores.”.

También, se propone la reforma de los artículos **32, 45, 269 y 274**, de la Ley General de Títulos y Operaciones de Crédito, y la derogación de los artículos **32, párrafo tercero, 45, numeral III, inciso c), 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191,192, 193, 194, 195, 196, 197, 198, 199, y 201**, del mismo ordenamiento.

De igual forma, se propone cambiar el nombre de *cheque de caja* a **título de pago de caja**. En esa tesitura, se formula la siguiente redacción al artículo **200**, de la Ley General de Títulos y Operaciones de Crédito:

“Artículo 200. Sólo las instituciones de crédito pueden expedir títulos de pago de caja, a cargo de sus propias dependencias. Para su validez éstas órdenes deberán ser nominativos y no negociables”.

Asimismo, se propone cambiar el nombre de *cheque de viajero* a **título de viajero**, y regularlo en un nuevo apartado en la Ley General de Títulos y Operaciones de Crédito; considerándolo como acto de comercio dentro de los supuestos que establece el artículo 75, del Código de Comercio. En esa tesitura, se propone la reforma a los artículos **202, 203, 204, 205, 206 y 207, párrafo segundo**, de la Ley General de Títulos y Operaciones de Crédito, para quedar de la siguiente forma:

“Artículo 202.- Los títulos de viajero son expedidos por el librador a su propio cargo, y pagaderos por su establecimiento principal o por las sucursales o los corresponsales que tenga en la República o en el extranjero. Los títulos de viajero pueden ser puestos en circulación por el librador, o por sus sucursales o corresponsales autorizados por él al efecto.”.

“Artículo 203. Los títulos de viajero serán precisamente nominativos. El que pague el título deberá verificar la autenticidad de la firma del tomador, cotejándola con la firma de éste que aparezca certificada por el que haya puesto los títulos en circulación.”.

“Artículo 204. El tenedor de un título de viajero puede presentarlo para su pago, a cualquiera de las sucursales o corresponsales incluidos en la lista que al efecto proporcionará el librador, y en cualquier tiempo mientras no transcurra el señalado para la prescripción.”.

“Artículo 205. La falta de pago inmediato dará derecho al tenedor para exigir al librador la devolución del importe del título de viajero y la indemnización de daños y perjuicios, que en ningún caso serán inferiores al 20% del valor del título no pagado.”.

“Artículo 206. El corresponsal que hubiere puesto en circulación los títulos de viajero, tendrá las obligaciones que corresponden al endosante y deberá rembolsar al tomador, el importe de los títulos no utilizados que éste le devuelva.”.

“Artículo 207. (...) “Las acciones contra el que expida o ponga en circulación los títulos de viajero, prescriben en un año a partir de la fecha en que los títulos son puestos en circulación.”.

En ese sentido, se propone la reforma de la **fracción XXVI**, al artículo **75**, del Código de Comercio, para quedar con el siguiente texto:

“Art. 75. La ley reputa actos de comercio:- - XXVI. Los títulos de viajero.”

De igual manera, se proponen las reformas de los artículos **1414 Bis-17, fracción III, inciso c)**, del Código de Comercio; **20, séptimo párrafo, 22-B, párrafo segundo, 29-C, primer párrafo, fracciones I, III, y V, párrafo cuarto, 32-B, fracción I, 59, fracciones IV y VI, 84-A, fracción I**, del Código Fiscal de la Federación; **1º-B, segundo y tercer párrafos, 5º, fracción II, y 34**, de la Ley del Impuesto al Valor Agregado; **2, párrafo quinto, 6º, fracción III, párrafos primero y segundo**, de la Ley del Impuesto Empresarial a Tasa Única; **24, fracciones III, VII, primer párrafo, y IX, 119-E, fracción XIV, segundo párrafo, 119-Ñ, fracción IV, párrafo tercero, 123, fracción I, 136, fracciones IV, párrafos primero, segundo y tercero, X, párrafo primero, y XIX, párrafo primero**, de la Ley del Impuesto Sobre la Renta; **58, fracción II, segundo párrafo**, de la Ley Federal para la Administración y Enajenación de Bienes del Sector Público; y, **3º, fracción XII, 4 Bis, fracción III, inciso c), 16, párrafo primero, y 48, fracción II**, de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros.

Por otra parte, se propone la derogación de los artículos **482, primer párrafo**, y **483**, del Código Federal de Procedimientos Civiles; **21, séptimo párrafo, 32-B, fracción II, 84-A, fracción II, 84-B, fracción II, y 105, último párrafo**, del Código Fiscal de la Federación; **387, fracción XXI**, del Código Penal Federal; **231, fracción XIII**, del Código Penal para el Distrito Federal; y, **16, párrafo segundo**, de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros.

En ese orden de ideas, se establece el siguiente articulado en materia de cheque electrónico, mismo que se propone se adicione en un diverso apartado relativo a los Títulos Valores, en la Ley General de Títulos y Operaciones de Crédito.

Del cheque electrónico.

ARTICULO 175. El cheque electrónico es un título valor con fines de instrumento de pago, que técnicamente consiste en un mensaje de datos enviado por el emisor al correo electrónico del destinatario, quien a su vez renvía el documento electrónico con su firma electrónica avanzada a la institución bancaria intermediaria, para que ésta previa verificación de su identidad, libre los fondos a la cuenta bancaria del destinatario.

ARTÍCULO 176. El cheque electrónico tiene las características de un cheque certificado para abono en cuenta; por lo que, ha de ser nominativo, no negociable y, por ende, no endosable.

ARTÍCULO 177. El cheque electrónico no producirá efectos de título de crédito, sino de forma de pago. Cualquier inserción en contrario se tendrá por no puesta.

El cheque electrónico sólo podrá ser emitido por quien, teniendo fondos disponibles en el intermediario, sea autorizado por éste para emitir cheques electrónicos a su cargo, y cuente con un certificado de firma electrónica avanzada vigente, expedido por un prestador de servicios de certificación, constituido conforme a lo dispuesto en el artículo 102 del Código de Comercio.

Dicha autorización se entenderá conferida al emisor que previamente haya solicitado a la institución bancaria intermediaria la certificación del cheque electrónico.

ARTICULO 178. El cheque electrónico debe contener:

I.- La mención de ser cheque electrónico, inserta en el documento electrónico;

II.- El lugar, fecha y hora en que se emite;

III.- La orden incondicional de pagar una suma determinada de dinero;

IV. El nombre del intermediario.

V. El nombre del destinatario;

VI. La cuenta bancaria del destinatario;

VII. El nombre del banco receptor;

VIII. La CLABE o cuenta bancaria estandarizada del destinatario;

IX.- La firma electrónica avanzada del emisor.

Los requisitos marcados con el VII y VIII, se indicarán en caso de que el cheque contenga la orden de depositarlo en otro banco.

ARTÍCULO 179. El emisor deberá enviar el documento encriptado con la llave pública del destinatario, quien podrá desencriptarlo con su llave privada. El emisor y el destinatario deberán acordar sobre el acuse de recibo del mensaje de datos, por lo que el destinatario está obligado a acusar recibo en la forma determinada con el emisor.

ARTICULO 180. El destinatario deberá renviar el cheque electrónico encriptado al intermediario para su pago, con su firma electrónica avanzada para su identificación.

ARTÍCULO 181. El intermediario luego de verificar las firma electrónica avanzada del emisor y destinatario, deberá librar los fondos que respalde el cheque electrónico a la cuenta bancaria del destinatario.

ARTÍCULO 182. El destinatario tiene el plazo de veinticuatro horas, a partir de que éste reciba el cheque electrónico en su cuenta de correo electrónico, para el cobro de dicho documento. En caso contrario, deberá reenviar el cheque electrónico no cobrado nuevamente al emisor quien lo archivara conforme al sistema establecido, para su ulterior consulta.

ARTÍCULO 183. El emisor, en caso de no ser presentado el cheque electrónico en el plazo indicado, podrá revocar el cheque, oponerse a su pago, y disponer de dichos fondos para la emisión de otro cheque electrónico.

ARTICULO 184. El cheque electrónico será siempre pagadero al momento del recibo del documento electrónico a la cuenta de correo electrónico del intermediario.

ARTICULO 185. El pago de un cheque electrónico deberá ser siempre en su totalidad. Cualquier inserción en contrario se tendrá por no puesta.

Cuando, sin justa causa, se niegue el intermediario a pagar un cheque electrónico, resarcirá al destinatario los daños y perjuicios que con ello le ocasione. En ningún caso la indemnización será menor del veinte por ciento del valor del cheque.

Las acciones contra la institución intermediaria en éste supuesto, prescriben en seis meses, contados a partir de la fecha en que concluya el plazo de presentación.

ARTICULO 186. La muerte o la incapacidad superveniente del emisor, no autorizan al intermediario para dejar de pagar el cheque electrónico.

ARTICULO 187. La declaración de que el emisor se encuentra en estado de concurso, no obliga al intermediario, desde que tenga noticia de ella, a rehusar el pago.

GLOSARIO

Audio. Es aquella información en forma de sonido perceptible al oído humano.

Bienes informáticos. Son todos aquellos elementos que forman el sistema – ordenador- en cuanto al hardware, ya sea la unidad central de proceso o sus periféricos, y todos los equipos que tiene una relación directa de uso con respecto a ellos y que, en su conjunto, conforman el soporte físico del elemento informático, así como los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático.

Bit. Se considera la unidad básica de medición de la información. A la electrónica capaz de procesar la información en forma de bits, se le conoce como electrónica digital. Para hacer referencia a la cantidad de información digital es más común utilizar el término bite. Un byte es un conjunto de 8 bits. Cuando la información es cuantiosa, se utilizan otras unidades de medición, el megabyte (MB), que equivale a un millón de bytes y el gigabyte, que equivale a mil millones de bytes.

Bit-tax. Es el “impuesto sobre el bit”.

Bomba lógica o cronológica. Exige habilidades especializadas ya que requiere programar la destrucción o modificación de datos en un futuro. A diferencia de los virus o los “gusanos”, las bombas lógicas son difíciles de detectar antes de que exploten. Su detonación puede programarse para que cause el máximo daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. También se utiliza como medio de extorsión. Su efecto es un daño –borrado o

destrucción de ficheros- en tiempo posterior –con retardo- al momento de su introducción.

Business to Business (B2B). Es una modalidad a través de la cual se consolida la comunicación entre empresas y se desarrolla confianza por la seriedad y compromiso que transmiten; pues, a través de esta categoría de negocio, se maximiza el grado de satisfacción entre las empresas partes, y beneficia de forma adicional a los concertantes en la disminución de costos, y en la edificación de nuevas formas de hacer negocios.

Business to Consumers (B2C). Refiere a la relación entre empresa y consumidor, la cual inicia a través de la investigación de mercado en línea, cuyo resultado advierte cuáles son las necesidades del comprador, para así, estar en aptitud de ofrecer los bienes y servicios que exactamente requiere.

Business to Administration (B2A). Bajo esta apertura comercial, se interrelacionan las personas y la administración pública, tal es el caso, de la información que ofrecen los gobiernos a través de sus páginas web, u organismos públicos, que ofrecen información al usuario.

Caballo de Troya. Consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Cajeros Electrónicos. Sistema de dinero electrónico que permite al cliente depositar dinero en una cuenta en una entidad de Interne, para efecto de poder usar ese dinero para adquirir bienes o servicios por Internet con un código alfanumérico asociado a su identidad (sus datos personales proporcionados a la entidad), que le permita adquirir, de los vendedores asociados a las entidades, bienes o servicios.

Centro de Arbitraje y Mediación de la Organización Mundial de la Propiedad Intelectual. Tiene su sede en Ginebra, Suiza, y fue creado en 1994. Es una

dependencia administrativa de la Oficina Internacional de la Organización Mundial de la Propiedad Intelectual (OMPI) y miembro de la Federación Internacional de Instituciones de Arbitraje Comercial (IFCAI). Ofrece servicios de arbitraje y mediación en relación con controversias internacionales comerciales entre partes privadas. Se le ha reconocido como uno de los principales proveedores de servicios de solución de controversias referentes a las controversias que plantean el registro y el uso de los nombres de dominio, y lo relacionado con la solución de controversias en materia de propiedad intelectual e Internet. Actualmente, este centro de arbitraje presta sus servicios al Application Service Provider Industry Consortium, consorcio internacional no lucrativo formado por más de 400 de las principales empresas mundiales dedicadas a las tecnologías de la información, a fin de elaborar prácticas y directrices para prevenir y solucionar las controversias internacionales. El centro recibe apoyo de una comisión consultiva y del Consejo de Arbitraje de la OMPI, ambos integrados por expertos de alto nivel.

Certificado digital. Es un mensaje de datos firmado electrónicamente que vincula a una entidad identificada plenamente ante un prestador de servicios de certificación, con una llave pública que ha sido generada por dicho PSC.

Cheque electrónico. En sentido estricto, el cheque electrónico es un mensaje de datos que contiene la orden incondicional de pagar a la vista una suma determinada de dinero, emitido al destinatario, a cargo de una institución de crédito. En sentido amplio, el cheque electrónico es una forma de pago consistente en un mensaje de datos enviado por el emisor al correo electrónico del destinatario (acreedor), quien a su vez envía el documento electrónico con su firma electrónica avanzada al intermediario (institución bancaria), para que éste previa verificación de la identidad de aquel, libre los fondos a su cuenta bancaria.

Cheque sustituto. Es una imagen digital del cheque original. Contiene la misma información que un cheque original, y siempre incluye un texto que lo identifica como una copia legal del cheque original: “This is a legal copy of your check. You can use it the same way you would use the original check” (en español: Ésta es una

copia legal de su cheque. Puede usarlo de la misma forma en que usaría el cheque original”).

Cibercorte en Michigan. Surge a través del gobernador John Engler, quien firmó a principios de 2002, un decreto para establecer en Michigan, Estados Unidos, una cibercorte independiente para los casos relativos a empresas de alta tecnología. Es una nueva forma de llevar los procesos; ello, en línea, donde surgen las teleconferencias, o conferencias vía e-mail, asimismo, las audiencias pueden celebrarse en cualquier momento del día.

Ciberjusticia. Es impartida por cibertribunales, en donde se ventilan los juicios en línea, con apoyo de las tecnologías de información y comunicación.

Crackers. Toda persona que por medios informáticos y de telecomunicaciones, accede a sistemas de información que le son vedados, con la intención de provocar un daño o apoderarse indebidamente de información.

CyberTribunal. Era un proyecto experimental elaborado por el Centre de Recherche en Droit Publique (CRDP, por sus siglas en francés), de la Universidad de Montreal, en septiembre de 1996. Era el de mayor apertura. No se erigía un juez, sino de moderaba el diálogo entre las partes a través de la mediación. El proyecto terminó en diciembre de 1999.

Cibertribunal de Lieja (Bélgica). Proyecto fue propuesto a la Fundación Rey Baudouin a finales de 2000, a iniciativa de la barra de abogados de dicha ciudad (Justicia en movimiento).

Comercio electrónico. Es la actividad comercial, que comprende transacciones de bienes y servicios, así como el flujo de información, a través de medios electrónicos.

Contrato electrónico. Es un contrato celebrado mediante dispositivos automáticos, principalmente por Internet; ya sea de forma directa o indirecta.

Contrato informático. Es el convenio que produce o transfiere las obligaciones y derechos sobre bienes o servicios informáticos. Como cualquier contrato, el contrato informático para que sea existente y válido, debe reunir los elementos que citan tales numerales.

Correo electrónico. Es un servicio que se clasifica dentro de los servicios de valor agregado, entendiéndose éstos como aquellos que emplean una red pública de telecomunicaciones y que tienen efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida por algún usuario y, que comercializan a los usuarios información adicional, diferente o reestructurada, o que implican interacción del usuario con información almacenada; ello, atento al artículo 3º, fracción XII, de la Ley Federal de Telecomunicaciones.

Datos de creación. Son códigos o claves criptográficas privadas, generados de manera secreta por el firmante, quien los utiliza para crear su firma electrónica al aplicar su llave privada, con el fin de lograr el vínculo entre dicha firma y su titular. Deberán ser tramitados por los contribuyentes (persona moral), ante el Servicio de Administración Tributaria (SAT). Cuando se traten de un contribuyente (persona física), ésta podrá tramitarlo ante dicha Administración, o bien, ante cualquier prestador de servicios de certificación (PSC) autorizado por el Banco de México.

Delito informático. Es el acto u omisión que sancionan las leyes penales, relacionados con las técnicas destinadas al tratamiento lógico y automatizado de la información. El bien jurídico que tutela es el patrimonio. Es “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Derecho informático. Es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica), y como objeto de estudio (derecho de la informática).

Derecho de la informática. Es el sistema de normas que regulan a la informática, entendida ésta como la ciencia del tratamiento automatizado de la información.

Destinatario. Se ha de entender la persona con la cual el iniciador tiene la intención de comunicarse mediante la transmisión del mensaje de datos, por oposición a cualquier persona que pudiera recibir, retransmitir o copiar el mensaje de datos en el curso de la transmisión.

Digitalización. Cuando la información se digitaliza, se somete a un proceso de conversión de su representación tradicional a un formato binario (bits), utilizando ciertos patrones o reglas que toman diversas muestras lo suficientemente significativas para reconstruir posteriormente la información sin perder el mensaje original. La información en forma de bits, se puede expresar a través de los siguientes: texto, gráfico, audio, video.

Dinero on line. Requiere interactuar con el banco (por módem o red) para llevar a cabo una transacción con una tercera parte. Esta modalidad incluye las tarjetas de crédito y el Saf-T-Pay.

Dinero off line. Se dispone del dinero en la propia computadora y puede gastarse cuando se desee, sin necesidad de contactar para ello con un banco. Dentro del dinero *off line*, se encuentra:

Directiva Europea sobre Comercio Electrónico. Hace referencia a la solución extrajudicial de litigios y dispone en su apartado primero que los Estados miembros velarán, para que en el caso de desacuerdo entre un prestador de servicios de la sociedad de la información y el destinatario de aquéllos, su legislación permita utilizar de manera efectiva mecanismos de solución extrajudicial, incluso mediante vías electrónicas adecuadas.

Documento electrónico. También llamado mensaje de datos. Es aquella información que se enseña o expresa, a través de un medio electrónico. Técnicamente, el documento electrónico, es “un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que, sometidos a un adecuado proceso, permiten su traducción a lenguaje natural mediante una pantalla o una impresora. Formado por la computadora o dispositivo electrónico, a través de sus propios órganos de salida, y que es perceptible por el hombre sin la necesidad de máquinas traductoras. Son aquellos documentos cuyo soporte se encuentra en medios electrónicos, llámese mensajes de datos, registro contable electrónico o el texto electrónico de un contrato. Es cualquier representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser asimilados en forma humanamente comprensible.

Documentos informáticos sobre soporte de papel. Son documentos producidos por medio de la computadora, creados mediante el uso de un periférico de salida (impresora), y se le dota de soporte papel para ser leído.

Documentos informáticos sobre soporte electrónico. Son documentos producidos en la computadora, que pueden ser leídos con la aplicación de la técnica informática. Sólo tiene un soporte electrónico o soporte informático

e-administración o administración electrónica. Hace referencia a aquellos mecanismos electrónicos que permiten la prestación de servicios públicos de la administración a ciudadanos y a empresas.

e-Cash. En funcionamiento desde 1994. Es un concepto de pago que surge de la firma Digicash. Es un software que adquiere el usuario. No tiene apariencia física. La compañía pionera que provee este servicio es eCash Technologies, Inc. Esta modalidad se emplea en micropagos, en donde la transacción permite mantener el anonimato del usuario y tener seguridad de autenticidad en virtud al uso de las firmas electrónicas. Los tres elementos que la integran son: el banco emisor, que valida la transacción y que cambia dinero real en virtual; los compradores, que obtienen su tarjeta prepago en el banco en el cual tiene una cuenta aperturada; y, los vendedores, que aceptan el e-cash. Como desventajas de esta modalidad se encuentra que, no

todos los bancos están afiliados al sistema Digicash, ni tampoco todos los comercios virtuales; por tanto, se debe navegar en busca de quien acepte esta clase de dinero; no obstante, los beneficios son más.

e-democracia o democracia electrónica. Permite la participación ciudadana en las decisiones políticas, a través de las TIC (nuevas tecnologías de información y comunicación), como lo es el voto electrónico.

e-gobierno o gobierno electrónico. Abarca todos los servicios en línea en la prestación de servicios públicos.

e-Resolution. Fundado en 1999. Se utiliza para la solución en línea de litigios relativos a los nombres de dominio. Inauguró su primer servicio de solución en línea de deferencias el 1 de enero de 2000, cuando recibía la acreditación de la Corporación Internet para Nombres y Números Asignados (ICANN). La plataforma tecnológica de eResolution ha permitido resolver varios cientos de asuntos con alcance mundial.

Encriptación. Es un proceso mediante, el cual, la información se convierte en algo completamente indescifrable para cualquier persona que no sea el destinatario o el propietario. Es una técnica que permite proteger la información al transformar los datos en algo totalmente incompresible y reconstruirlos después cuando así se requiera. Para realizar el proceso de encriptación es necesario además del mensaje o documento a encriptar, un valor independiente llamado llave de encriptación. Cuando se descripta necesitamos otro valor, que en este caso de le llama llave de descriptación. Este proceso es en realidad una operación matemática sobre un número entero utilizando números primos. Es necesario recordar que los números primos son aquellos divisibles sólo por sí mismos y por la unidad; por ejemplo, 2,3,5,7,11,13,17,19,23,29,31. Por definición se trata de números naturales por lo que únicamente pueden ser números enteros positivos y son infinitos. Segundo, la operación matemática llamada módulo (mod) se define como el número entero (sin decimales) que resulta de la división entre dos números, es decir: $a \text{ mod } b = \text{entero}$ (sin decimales) resultante de a/b . En términos generales el método de encriptación

utilizado en la firma electrónica avanzada se centra en la obtención de dos números primos (p,q) del mismo tamaño, que multiplicados entre sí dan por resultado un número entero (n). En conjunto (p,q) se conoce como llave privada y (n) como llave pública, y se utilizan siempre números enteros bastante grandes, tales como números de 308 dígitos expresados en 1024 bits.

Encriptación asimétrica. Ocurre cuando la llave de encriptación, es diferente a la llave de desencriptación. En este caso dichas llaves son llamadas pública y privada. A este método se le conoce como PKI (Public Key Infrastructure). El método asimétrico es el indicado para la implementación de la firma electrónica.

Encriptación simétrica. Sucede cuando la llave de encriptación y la llave de desencriptación son idénticas.

Ergonomía informática. Proviene de ergon, que significa energía, trabajo; nomos, que significa tratado; y, del vocablo informática, que es el conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información. Es el conjunto de implicaciones de orden normativo-laboral provocadas por el uso de la informática; ejemplo de ello, la movilización de puestos (desplazamiento laboral), y las condiciones de trabajo (jornada de trabajo, vacaciones, salario).

Fax. Es un medio electrónico por medio del cual se envía información, a través de un dispositivo de comunicación con que cuenta, que transmite imágenes y textos a través de una línea telefónica. Implica el uso de escáner (escandidor), un módem y una impresora; tiene la capacidad de leer una hoja de papel, convirtiendo cada punto en un código numérico. Parecido que un módem, puede convertir estas señales digitales en otro tipo de señal apropiado para viajar por una línea telefónica hasta la máquina del fax del destinatario. Al igual que una impresora, recibe las señales para imprimir puntos en la misma posición que estaba la hoja original.

Firma. Nombre y apellido, o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad o para obligarse

a lo que en él se dice.”.

Firma electrónica. Se entenderá los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

Firma electrónica avanzada. Es un conjunto o bloque de caracteres, códigos o claves criptográficas privadas en forma electrónica, que viaja junto, asociado o anexo a un documento digital, y mediante el cual se acredita quién es el autor o emisor del mismo.

Firma digital. Es una *especie* de la firma electrónica. Es un bloque de caracteres que acompaña a un documento o archivo, y acredita quién es el autor (autenticación) del mismo, y que no ha existido ninguna manipulación posterior de los datos (integridad). Se trata de cierto tipo de firma electrónica basada en el uso de criptografía; la más comúnmente utilizada es la llamada criptografía asimétrica o de llave pública. Puede ser definida como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación de un algoritmo (fórmula matemática) de cifrado asimétrico o de llave pública, a un mensaje determinado. Este algoritmo equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje. Asimismo, esta firma permite determinar de forma fiable que el emisor del mensaje de datos es realmente la persona que dice ser, así como si el contenido del documento ha sido alterado o no posteriormente; esto es, permite asegurar la identidad del firmante y la integridad del mensaje. Desde el punto de vista tecnológico, la firma digital es una cadena o secuencia de caracteres que se adjunta o asocia al final del cuerpo de un mensaje. La firma digital se crea mediante el uso de la criptografía de llave pública.

Foro de Arbitraje Nacional (NAF). Fundado en 1986 en Minneapolis, Minnesota, notable por su neutralidad en la toma de decisiones y la aplicación de leyes

sustantivas para resolver casos de arbitraje. Obtuvo la aprobación como un proveedor de servicio para la resolución de disputas por ICANN el 23 de diciembre de 1999.

Función Hash. Proceso matemático de obtener un resumen único de tamaño fijo y pequeño.. El algoritmo asimétrico tiene el inconveniente de ser lento, por lo que, no es útil para aplicarlo en todos los casos para cifrar mensajes digitales, en especial si son éstos de gran tamaño; toda vez que, entre más grande sea el mensaje más lento es el proceso de encriptación asimétrico. Por ello, se ha utilizado una función matemática que produce un resumen o compendio de tamaño pequeño y fijo, sin importar el tamaño del mensaje original; posteriormente, se aplica la encriptación a dicho resumen. Esta función garantiza que no se encuentren dos mensajes diferentes que generen un resumen idéntico, aun cuando la diferencia de ambos sea de sólo un signo de puntuación.

Gráfico. Es aquella información expresada en forma de imagen estática de un solo color o multicolor.

“Gusanos”. se fabrican de forma análoga al virus con miras a infiltrarlos en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

Iniciador. Es la persona que genera el mensaje de datos aun si el mensaje ha sido transmitido por otra persona.

Información. Es todo conjunto de datos representados de forma escrita, gráfica, auditiva o visual, que ofrece un conocimiento o pensamiento. El autor Claude Shannon, precursor de la teoría de la información, quien dándose cuenta de las cualidades poco atractivas de la palabra información, en 1948, tituló su artículo “Una teoría matemática de la comunicación”, en la que pronuncia que cuanto mayor y mejor sea la información, menor será el desconocimiento en las personas. En esta publicación quedó demostrado que la información (la voz de las personas, las conversaciones telefónicas, las emisiones de radio y la televisión, la telegrafía, las

publicaciones escritas, etcétera), puede ser medida y cuantificada.

Informática jurídica. Es el conjunto de aplicaciones de la informática en el ámbito del derecho. Es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como a la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación”.

Informática jurídica documentaria. Es el área más antigua de la informática jurídica. En los sistemas de informática jurídica documentaria se trata de crear un banco de datos jurídicos o corpus jurídico documentario, relativo a cualquiera de las fuentes del derecho, excepto la costumbre; cuyo rendimiento está en función de la exactitud y extensión de los datos contenidos y de los criterios de búsqueda de los documentos (leyes, acuerdos, reglamentos doctrina, jurisprudencia). Los batch, fueron los primeros sistemas de interrogación de bancos de datos jurídicos, que permitían la búsqueda en los archivos, esto es, de textos y de palabras ordenadas alfabéticamente, que indicaban, una vez señalada una palabra, la “dirección” donde estaba almacenada..

Informática jurídica metadocumentaria. Es un tipo de aplicación de la informática que va más allá de un banco de datos jurídicos, pues incorpora la asistencia máxima al usuario en sus distintas vertientes: decisional, educativa, investigación, previsión y redacción.

Informática jurídica de control y gestión. El aspecto documentario no es el único que se ha desarrollado dentro de la informática jurídica, pues otras áreas desde hace tiempo se desarrollan, como lo es la llamada informática jurídica de control y gestión, cuyo antecedente se remonta al tratamiento de textos jurídicos mediante el uso de procesadoras de palabra, así como las experiencias emanadas en materia de automatización de registros públicos. Esta rama alcanza fundamentalmente los ámbitos jurídico-administrativo, judicial, registral y despachos de abogados.

Instituto para la Resolución de Conflictos (CPR). Fundada en 1999; es una alianza no lucrativa constituida por organismos multinacionales y despachos prestigiosos para ofrecer a empresas e instituciones públicas una alternativa. Formado por 500 asesores legales de las mayores empresas, socios de los mejores despacho, catedráticos notables e instituciones públicas seleccionadas. Su manera de actuar es a través de los llamados paneles de neutralidad y mediación. Incluye en su programa extensas publicaciones: libros, videos, modelos de procedimiento de resolución de conflictos y herramientas prácticas en más de 20 áreas tanto sustantivas como procedimentales, así como modelos formales y sus cláusulas respectivas.

Intercambio electrónico de datos (EDI). Es un medio electrónico utilizado para generar, enviar, recibir o archivar información. Sus siglas corresponden al inglés Electronic Data Interchange. Los tres componentes de un sistema EDI son los mensajes estándar, los programas EDI o las estaciones de usuario, y las (tele)comunicaciones. El EDI es el envío y recepción de documentos a través de medios telemáticos con el propósito de posibilitar su tratamiento automático. Está considerado este medio como un servicio de valor agregado, en virtud de que proporciona a los usuarios el almacenamiento y envío automatizado de información estructurada bajo un formato definido. Como ejemplo, el intercambio electrónico de datos (EDI) se utiliza en operaciones masivas como órdenes de compra, pedidos, facturación y suscripciones, las cuales permiten a las empresas agilizar, incrementar y facilitar sus operaciones, suprimir grandes costos de papel, ampliar su prestigio, analizar mercados y perspectivas de clientes, etcétera.

Intermediario. En relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

Internet. Es una infraestructura constituida por protocolos que permite el enlace de computadoras por todo el mundo, la cual, no obstante se concibió como un sistema descentralizado, y aparentemente bajo sin ninguna autoridad o gobierno central que lo

regule, lo cierto es que las conductas llevadas a cabo con ayuda de esta red no están exentas del cumplimiento de la norma jurídica; ello, en virtud de que se encuentra sometida a una jurisdicción, competencia, y legislación aplicable. Es una federación de redes. Es una infraestructura compartida constituida por protocolos que enlaza computadoras por todo el mundo, a través de mecanismos y protocolos, que permiten conectar usuarios entre sí, por medio de proveedores de servicios.

Justicia, significa, dar a cada quien lo que le corresponde.

Micropagos. es utilizado como alternativa económica a los medios de pago con tarjeta, basados en la existencia de cupones electrónicos que representan dinero con los que el comprador paga al vendedor.

Nombres de dominio. Es el nombre asociado a un sitio o lugar en la red; esto es, “un medio de identificación y ubicación en el Internet”,

Ofimática jurídica. Es la automatización de las oficinas con actividades jurídicas, o llamada, ha simplificado las labores propias de los despachos de abogados, mediante el uso de sistemas automatizados como control de asuntos con horarios, redacción de escritos, actualización de criterios jurisprudenciales, doctrina, bibliografía, etcétera.

On line Ombuds Office (Oficina de Mediadores en Línea). Es una iniciativa del Center for Information Technology and Dispute Resolution de la Universidad de Massachusetts. Desde 1996, esta oficina ofrece sus servicios de mediación particularmente en asuntos relacionados a litigios entre miembros de un grupo de debate, competidores, entre proveedores de acceso a Internet, y relacionados con propiedad intelectual. El proyecto se prosigue en la actualidad.

Outsourcing. Cesión de la gestión de los sistemas de información de una entidad a un tercero.

Piratas Informáticos o hackers. Es la persona que accede a una computadora de forma no autorizada e ilegal, valiéndose de medios informáticos y de telecomunicaciones. Su motivación es el simple deseo de quebrantar el sistema como desafío propio. A menudo se hacen pasar por usuarios legítimos del sistema.

Política informática. Trata con el adecuado desarrollo de la industria de construcción de equipos de cómputo y de programación, planeación, difusión y aplicación del fenómeno informático, la contratación gubernamental de bienes y servicios informáticos; la formulación de normas y estándares en materia informática, así como el control de importaciones y exportaciones sobre equipos accesorios y programas de computadoras.

Legislación informática. Es un sistema de normas que emanan del uso de la informática que regulan diversas áreas, entre otras, a saber: protección de la información y de los datos personales; regulación jurídica del flujo internacional de datos; regulación jurídica de Internet; propiedad intelectual y las nuevas tecnologías de la información y comunicación; contratos informáticos; spam; aspectos laborales de la informática; documentos electrónicos o informáticos y su valor probatorio; las cuales en lo conducente se exponen a continuación:

Medios ópticos o similares. Refiere a cualquier medio por el que se pueda generar, enviar, comunicar, archivar o conservar mensajes de datos, además de los ya conocidos, como el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

Netcash. Es un sistema similar al e-cash, desarrollado por el Sciences Institute of the University of Southern California, y consiste en un mecanismo conectado a varios servidores de moneda (currency servers) que hacen posible cambiar en dinero electrónico algunas otras formas de pago, como los cheques electrónicos.

Phreaker. Es la persona que para llevar a cabo la actividad de hacker o de cracker, utiliza indebidamente líneas telefónicas, que más allá del valor de los pulsos

telefónicos utilizados, su motivación es evitar ser rastreado por el software específico diseñado para tal efecto.

Prestadores de servicios de certificación en materia mercantil. Es la persona o institución pública que presta servicios relacionados con firmas electrónicas y que expide los certificados, en su caso.

Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que utilizan para ello, son: virus, “gusanos”, y bomba lógica o cronológica, las cuales se describen a continuación:

Saf-T-Pay. Es un sistema de pago que sin necesidad de un nuevo instrumento o clave, una vez que el cliente elige una compra. *Saf-T-Pay* facilita la cantidad en moneda local y el pago electrónicamente por medio de su banco.

Sello digital. Es un mensaje electrónico que acredita que un documento digital fue recibido por la autoridad correspondiente; es decir, cuando los contribuyentes remitan un documento digital a las autoridades fiscales, recibirán el acuse de recibo que contenga el sello digital.

Servicios informáticos. Son todos aquellos que sirven de apoyo y complemento a la actividad informática en una relación de afinidad directa con ella.

Sistemas sin tarjeta. Es dinero electrónico en sentido estricto. Se substituye el soporte tradicional por el soporte electrónico, esto es sustituyendo el papel por bits. El medio de pago creación del criptógrafo David Chaum basado en Software que permite a sus usuarios enviar dinero electrónico en pago de las compras realizadas desde cualquier ordenador a otro, utilizando cualquier red de comunicación, incluida Internet, y que pretende preservar el anonimato del comprador.

Software. Ficheros, programas, aplicaciones y sistemas operativos que nos permiten

trabajar con la computadora o sistema informático. Se trata de los elementos que hacen funcionar al hardware.

Spam. La palabra *spam*, surge de la contratación de los productos de comida enlatada llamada **Shoulder Pork and hAM/SPiced hAM** (spam), que era enviada de forma masiva a las tropas estadounidenses durante la Segunda Guerra Mundial. De ahí deriva el concepto Spam, para referirse a la práctica de enviar correo de manera indiscriminada a través de la red de Internet, sin importar el receptor final del correo, esto es, un modo masivo de publicitar productos o servicios.

Square Trade. Fundado en 1999. Funciona en mayor apego en el sector de comercio electrónico entre consumidores C2C. El procedimiento es amistoso, en el sentido de su informalidad. Primeramente, el comprador o el vendedor presentan una queja a Square Trade, recopilando toda la información pertinente en un formulario electrónico. Seguido, se notifica a la contraparte por correo electrónico. Si se presenta una respuesta, este servicio permite a las partes el acceso a formularios en un sitio protegido, mediante contraseñas y nombre de usuario. En esta etapa las partes pueden tratar de resolver el litigio de forma amistosa, de lo contrario, podrán pedir a Square Trade, que designe un mediador, en cuyo caso deberán pagar un honorario bastante modesto. En caso de un arreglo, con o sin ayuda del mediador, la diferencia quedará solventada y se comunicará a las partes un documento en el que se consigna el acuerdo.

Tarjetas de Crédito. Es utilizada para pagar transacciones electrónicas. Tiene la ventaja de permitir al consumidor pagar en cualquier sitio web sin importar la moneda en que está expresando el importe, en virtud de que la conversión se realiza de manera automática. Cuentan con el estándar de encriptación SET (Secure Electronic Transaction), liderado por Visa y masterCard o por SSL (Secure Socket Layer) de Netscape Communications Corp, para evitar que al entregar el número de tarjeta en cada compra, se deje huella fácil de seguir y que permita recabar información acerca del consumidor.

Tarjetas monederos o monedero electrónico. Es una tarjeta que incorpora un chip

en el que se almacena un valor monetario prepagado que puede ser gastado en cualquier comercio con lector de tales tarjetas. El titular de la tarjeta puede cargarla de dinero en cualquier terminal de carga.

Técnica de salami. Es la variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

Teletrabajo. Es la “forma flexible de organización del trabajo, que consiste en el desempeño de la actividad profesional sin la presencia física del trabajador de la empresa durante una parte importante de su horario laboral. Es “una forma flexible de organización del trabajo que se realiza con ayuda de las tecnologías de la información y las comunicaciones, en un lugar distinto y alejado del que ocupa la organización o la persona para quien se realiza el trabajo. Es un conjunto de aparatos que sirven para transmitir despachos, o mensajes a larga distancia. Es un medio o tecnología similar a la utilizada en los medios electrónicos y ópticos, puesto que sirve para transmitir mensajes a larga distancia mediante impulsos eléctricos que circulan por un hilo metálico u óptico, o a través del viento en el caso de los inalámbricos.

Télex. Es un acrónimo de TELEprinter EXchange (intercambio entre teleimpresores). Es un servicio transmisor de mensajes mecanografiados mediante teletipos (telégrafos), que realizan directamente la transmisión de señales por teclado y la recepción en caracteres tipográficos. Este medio electrónico consta de un transmisor, un receptor y una central dotada de una computadora.

Texto. Es aquella información expresada en forma de caracteres alfanuméricos y una serie de signos de puntuación que pertenecen a cierto alfabeto conocido.

TIC. Nuevas tecnologías de información y comunicación.

Transferencia electrónica de fondos interbancarios. Envío electrónico de dinero de una cuenta de cheques o tarjeta de débito de un Banco a una cuenta de cheques o tarjeta de débito en cualesquiera de las instituciones bancarias ubicadas dentro del territorio nacional. Tanto quien envía y recibe la transferencia, deben contar con una

cuenta de cheques o una tarjeta de débito, lo que permite al cliente de un banco hacer pagos o enviar fondos desde su cuenta a una cuenta en otro banco, o bien, enviar una transferencia electrónica a una cuenta de cheques o ahorros de otro banco radicada en una sucursal en cualquier lugar del país.

Video. Es aquella información en forma de secuencias de múltiples imágenes perceptibles por la vista que transmiten la sensación del movimiento.

Virus. es una serie de claves programáticas que pueden adherirse a los programas informáticos y propagarse a otros. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como mediante el método caballo de Troya.

Virtual Magistrate. En marzo de 1996 se inauguró este proyecto, un servicio de arbitraje en línea resultante de la colaboración entre Cyberspace Law Institute (CLI) y el National Center for Automated Information Research (NCAIR). Su objetivo, era estudiar la manera de resolver las diferencias entre un usuario y un operador de redes, o entre usuarios. El ámbito de aplicación se limitaba a los conflictos generados por mensajes o ficheros con contenido ilícito. El procedimiento de arbitraje era voluntario y se efectuaba esencialmente por correo electrónico. Se denomina arbitraje contractual, en virtud de que surtía algunos efectos obligatorios, pero no tenía efectos ejecutorios con arreglo a las legislaciones y tratados sobre la materia. Este proyecto se prosigue bajo los auspicios de la Universidad Chicago Kent.

CONCLUSIONES

PRIMERA. La utilización de la tecnología en el mundo cumple su finalidad cuando quienes la adquieren participan de un buen entendimiento.

SEGUNDA. La Constitución Política de los Estados Unidos Mexicanos, señala que el derecho a la información será garantizado por el Estado; en ese sentido, considero que el Estado debe erigir los instrumentos para que las comunidades más apartadas

(comunidades indígenas), tengan acceso de manera gratuita a las tecnologías de información y comunicación. Es el tiempo de utilizar las tecnologías y aprovecharlas para edificar, ayudar y alcanzar, a aquellas poblaciones. Edificar, para que quienes se dediquen al comercio, puedan mostrar y vender sus productos a través de Internet a todo el mundo. Ayudar, a aquellos jóvenes que desean avanzar en sus estudios, a través de las escuelas y universidades en línea. Alcanzar, a dichas poblaciones para que estas tengan acceso a la información y comunicación.

TERCERA. Se propone la creación de la “Ley Federal contra actos de exhibicionismo corporal con fines lascivos o sexuales, en medios de comunicación impresos, visuales y auditivos, espectaculares, Internet, y demás tecnologías de información y comunicación”.

CUARTA. Se propone la regulación de la firma electrónica avanzada en la Constitución Política de los Estados Unidos Mexicanos, en donde se le dé plena validez, para efecto de que pueda ser utilizada en las resoluciones judiciales, y demás materias; y, en esa tesitura, se cumpla con la garantía prevista en el artículo 16, de la Carta Magna.

QUINTA. Se propone el cheque electrónico, cuya naturaleza sea de un cheque certificado para abono en cuenta.

SEXTA. Se propone la regulación del cheque electrónico, dada sus características de fiabilidad, elementos de seguridad, y provisión garantizada; además de que genera mayor circulación de moneda, ahorro de papel, y crecimiento económico. La experiencia de Estados Unidos de América indica los beneficios que representa el uso del cheque electrónico o “cheque sustituto” en su actual práctica bancaria.

SÉPTIMA. Formalmente, el cheque sobre papel es un título de crédito; no obstante, en atención a su naturaleza, no contiene un derecho de crédito, sino “un valor”; por lo que, se propone que el cheque electrónico se regule en la Ley General de Títulos y

Operaciones de Crédito, en un apartado denominado “Títulos Valores”; dado que este es un título valor con su finalidad de instrumento de pago.

OCTAVA. Se propone la adición del articulado que se formula relativo al “cheque electrónico”, en la Ley General de Títulos y Operaciones de Crédito; para su entrada en vigor a los 24 meses, contados a partir de la fecha de su publicación en el Diario Oficial de la Federación, considerándose como año de dicha publicación, la presente anualidad (2011). Dicho lapso de tiempo o *vacatio legis*, es con el objeto de que dichos dispositivos puedan ser conocidos suficientemente, antes de que adquieran fuerza obligatoria.

NOVENA. Se propone cambiar el nombre de *cheque de caja* a título de caja, y el nombre de *cheque de viajero* a título de viajero, ambos regulados en la Ley General de Títulos y Operaciones de Crédito; toda vez que éstos no reúnen las características propias del cheque. Dichas reformas se proponen para su entrada en vigor, a los 24 meses, contados a partir de la fecha de su publicación en el Diario Oficial de la Federación, considerándose como año de dicha publicación, la presente anualidad (2011).

DÉCIMA. Se propone la reforma de los numerales de los diversos ordenamientos que contengan al cheque, y que se ajusten a la forma del cheque electrónico, a efecto de cambiar la denominación de cheque a “cheque electrónico”; asimismo, se propone la derogación de los numerales que contengan al cheque y que no se ajusten a esta nueva forma de pago electrónico. Dichas reformas se proponen para su entrada en vigor, a los 24 meses, contados a partir de la fecha de su publicación en el Diario Oficial de la Federación, considerándose como año de dicha publicación, la presente anualidad (2011).

DÉCIMA PRIMERA. La ciberjusticia es un paso hacia una impartición de justicia pronta; ello, en virtud de la ayuda que ofrecen las nuevas tecnologías de información y comunicación. Por lo que, es contundente implementar los juicios en línea, para efecto de resolver de manera pronta sobre las pretensiones y excepciones de los

justiciables. Entre algunas particularidades de estos juicios, se encuentran que las partes no tendrán necesidad de acudir al órgano jurisdiccional, pues existirá un expediente electrónico, en donde a través de claves, contraseñas y su firma electrónica avanzada, éstos podrán acceder a un sistema de justicia en línea, y presentar sus escritos digitalmente; no será necesario que las partes exhiban copias para correr los traslados, salvo que hubiese tercero interesado; las notificaciones se practicarán a través de un sistema, previo aviso del Actuario a las partes mediante correo electrónico, de que existe una actuación o resolución en el expediente electrónico; en donde se tendrá como legalmente practicada la notificación, cuando el sistema genere el acuse de recibo electrónico donde conste la fecha y hora en que la o las partes notificadas ingresaron al expediente electrónico; asimismo, las pruebas documentales se digitalizarán, y en el caso de las pruebas confesional o testimonial, podrá utilizarse el método de videoconferencia.

DÉCIMA SEGUNDA. El hombre renueva su mente con la visión de un cambio en su vida. “Hacia adelante está la respuesta”. Nuestra nación necesita mirar hacia ese cambio que produce bienestar. La convicción generalizada de que el fenómeno globalizador es un detonante para el crecimiento económico, pondrá al mundo en una misma dirección y condiciones de desarrollo.

“Donde no hay dirección sabia, caerá el pueblo; Mas en la multitud de consejeros hay seguridad”.

BIBLIOGRAFÍA

Andrés Cárpoli, Gabriel, La Firma Electrónica en el Régimen Comercial Mexicano, editorial Porrúa Sociedad Anónima de Capital Variable, Primera edición, México, 2004.

Astudillo Ursúa, Pedro, Los Títulos de Crédito, editorial Porrúa, Sociedad Anónima

de Capital Variable, Séptima edición, México 2006.

Becerra Bautista, José, **El Cheque sin Fondos**, editorial Kino, Sociedad Anónima, Cuarta edición, Tijuana, B.C. 1973.

Bejarano Sánchez, Manuel, **Obligaciones Civiles**, Oxford University Press México, Sociedad Anónima de Capital Variable, Quinta edición, México 1999.

Castrillón y Luna, Víctor M., **Títulos Mercantiles**, editorial Porrúa, Sociedad Anónima de Capital Variable, Segunda edición, México, 2008.

Cavazos Arroyo Judith y Reyes Guerrero Soraya, **Comercio Electrónico: un enfoque de modelos de negocio**, editorial Grupo Editorial Patria, Sociedad Anónima de Capital Variable, Primera reimpresión, México, 2008.

Cervantes Ahumada, Raúl, **Títulos y Operaciones de Crédito**, editorial Porrúa Sociedad Anónima de Capital Variable, Décima Séptima edición, México, 2007.

Cisneros Farias, Germán, **La Interpretación de la Ley**, editorial Trillas, Sociedad Anónima de Capital Variable, México 2000.

Charles E. McLure, Jr. y Giampaolo Corabi, **La tributación sobre el comercio electrónico: objetivos económicos, restricciones tecnológicas y legislación tributaria**, Ediciones Depalma, Argentina, 2000.

Davara Rodríguez, Miguel Ángel, **Manual de Derecho Informático**, editorial Arazandi, Sociedad Anónima, Séptima edición, Navarra, 2005.

Dávalos Mejía, Carlos Felipe L., **Títulos y Operaciones de Crédito**, Oxford University Press México, Sociedad Anónima de Capital Variable, Tercera edición, México 2002.

De Pina Vara, Rafael, **Teoría y Práctica del Cheque**, editorial Porrúa, Sociedad Anónima de Capital Variable, Tercera edición, México, 1984.

Díaz Bravo, Arturo, **Títulos y Operaciones de Crédito**, IURE editores, Sociedad Anónima de Capital Variable Segunda edición, México 2006.

Domínguez del Río, Alfredo, **La Tutela Penal del Cheque**, editorial Porrúa, Sociedad Anónima de Capital Variable, Primera edición, México, 1974.

Escuti, Ignacio A., **Títulos de Crédito**, Tercera edición, Editorial Astrea de Alfredo y Ricardo Desalma, Buenos Aires 1992.

García Más, Francisco Javier, **Comercio y Firma Electrónicos (Análisis Jurídico de los Servicios de la Sociedad de la Información)**, editorial Lex Nova, Sociedad Anónima, Segunda edición, España, 2004.

García Maynez, Eduardo, **Introducción al Estudio del Derecho**, editorial Porrúa, Sociedad Anónima de Capital Variable, Quincuagésimo Primera edición, México, 2000.

Gil y S, José Pérez, **El cheque sin fondos**, Imprenta “Zavala” San Ildefonso y Carmen, México 1945.

Gómez Gordoa, José, **Títulos de Crédito**, editorial Porrúa, Sociedad Anónima de Capital Variable, Décima edición, México, 2007.

Joan Hortalà i Vallvé, Franco Roccatagliata y Piergiorgio Valente, **La fiscalidad del comercio electrónico**, Editorial CISS, Sociedad Anónima, Primera edición, Bilbao, 2000.

León Tovar, Soyla H., González García Hugo, **Derecho Mercantil**, Oxford University Press México, Sociedad Anónima de Capital Variable, México, 2007.

León Tovar, Soyla H., González García, Hugo, Vázquez del Mercado Blanco, Oscar, **La firma electrónica avanzada**, Oxford University Press México, Sociedad Anónima de Capital Variable, México, 2007.

Mantilla Molina, Roberto L., **Derecho Mercantil**, editorial Porrúa, Sociedad Anónima de Capital Variable, Décimo Cuarta reimpresión, México 2007.

Mantilla Molina, Roberto L, **Títulos de Crédito**, editorial Porrúa, Sociedad Anónima de Capital Variable, Segunda edición, México, 1983.

Martínez Alfaro, Joaquín, **Teoría de las obligaciones**, editorial Porrúa, Sociedad Anónima de Capital Variable, Décimo Primera edición, México, 2008.

Orizaba Monroy, Salvador, **El Cheque**, editorial SISTA, Sociedad Anónima de Capital Variable, Primera edición, México, 2005.

Paganoni O´ Donohoe, Francisco Raúl, **Teoría General de los Títulos de Crédito**, O.G.S. Editores, Sociedad Anónima de Capital Variable, Primera edición, México, 2003.

Reyes Krafft, Alfredo Alejandro, **La Firma Electrónica y las Entidades de Certificación**, editorial Porrúa, Sociedad Anónima de Capital Variable, Segunda edición, México 2008.

Rodríguez Rodríguez, Joaquín, **Curso de Derecho Mercantil**, editorial Porrúa, Sociedad Anónima de Capital Variable, Vigésimo Cuarta edición, México 1999.

Rojas Amandi, Víctor Manuel, **El uso de Internet en el derecho**, Oxford University Press México, Sociedad Anónima de Capital Variable, Segunda edición México, 2001.

Rojina Villegas, Rafael, **Teoría General de las Obligaciones**, Tomo III, editorial Porrúa, Sociedad Anónima de Capital Variable, Vigésimo Séptima edición, México, 2007.

Sánchez Miranda, Arnulfo, **Estrategias Financieras de los Impuestos**, Sistemas de Información Contable y Administrativa Computarizados, Sociedad Anónima de Capital Variable, Primera edición, México, 2000.

Sariñana, Enrique, **Derecho Mercantil**, editorial Trillas, Sociedad Anónima de Capital Variable, Primera edición, México 1999.

Téllez Valdés, Julio, **Derecho Informático**, editorial Mc Graw-Hill/Interamericana Editores, Sociedad Anónima de Capital Variable, Cuarta edición, México, 2009.

Tena, Felipe de J., **Derecho Mercantil Mexicano**, editorial Porrúa, Sociedad Anónima de Capital Variable, Vigésimo Primera edición, México 2006.

Universidad de los Andes, Facultad de Derecho, Internet, **Comercio Electrónico & Telecomunicaciones**, Universidad de los Andes, Facultad de Derecho, Legis Editores Sociedad Anónima, Primera edición, Colombia, 2002.

Valdeón, Julio, **La Baja Edad Media**, Red Editorial Iberoamericana, Sociedad Anónima (REI- México), México, 1988.

Viviana Sarra, Andrea, **Comercio electrónico y derecho**, Editorial Astrea de Alfredo y Ricardo Depalma, Argentina, 2000.

LEGISLACIÓN CONSULTABLE

CÓDIGO CIVIL FEDERAL. Código publicado en la Sección Tercera del Diario Oficial de la Federación los días sábado 26 de mayo; sábado 14 de julio; viernes 3 de agosto y viernes 31 de agosto, todos de 1928.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 28 DE ENERO DE 2010.

CÓDIGO CIVIL PARA EL DISTRITO FEDERAL. Código publicado en la Sección Tercera del Diario Oficial de la Federación los días sábado 26 de mayo; sábado 14 de julio; viernes 3 de agosto y viernes 31 de agosto, todos de 1928.

ÚLTIMA REFORMA PUBLICADA EN LA GACETA OFICIAL DEL DISTRITO FEDERAL: 27 DE ENERO DE 2011.

CÓDIGO DE COMERCIO. Código publicado en el Diario Oficial de la Federación, del lunes 7 de octubre al viernes 13 de diciembre de 1889.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 27 DE ENERO DE 2011.

CÓDIGO DE PROCEDIMIENTOS PENALES PARA EL DISTRITO FEDERAL. Código publicado en el Diario Oficial de la Federación, el sábado 29 de agosto de 1931.

ÚLTIMA REFORMA PUBLICADA EN LA GACETA OFICIAL DEL DISTRITO FEDERAL: 18 DE MARZO DE 2011.

CÓDIGO FEDERAL DE INSTITUCIONES Y PROCEDIMIENTOS ELECTORALES. Código publicado en la Cuarta Sección del Diario Oficial de la Federación, el lunes 14 de enero de 2008.

CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES. Código publicado en la Sección Segunda del Diario Oficial de la Federación, el miércoles 24 de febrero de 1943.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 30 DE DICIEMBRE DE 2008.

CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES Código publicado en la Sección Segunda del Diario Oficial de la Federación, el jueves 30 de agosto de 1934.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 30 DE NOVIEMBRE DE 2010.

CÓDIGO FISCAL DE LA FEDERACIÓN. Código publicado en el Diario Oficial de la Federación, el jueves 31 de diciembre de 1981.

ÚLTIMA ACTUALIZACION POR MISCELANEA FISCAL: 31 DE DICIEMBRE DE 2010.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 10 DE MAYO DE 2011.

CÓDIGO PENAL FEDERAL. Código publicado en la Tercera Sección del Diario Oficial de la Federación, el viernes 14 de agosto de 1931.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 10 DE MAYO DE 2011.

CÓDIGO PENAL PARA EL DISTRITO FEDERAL. Código publicado en la Gaceta Oficial del Distrito Federal, el martes 16 de julio de 2002.

ÚLTIMA REFORMA PUBLICADA EN LA GACETA OFICIAL DEL DISTRITO FEDERAL: 18 DE MARZO DE 2011.

ESTATUTO DEL SERVICIO FISCALIZADOR DE CARRERA DE LA AUDITORIA SUPERIOR DE LA FEDERACIÓN. Estatuto publicado en la Primera Sección del Diario Oficial de la Federación, el miércoles 3 de febrero de 2010.

ESTATUTO DEL SERVICIO PROFESIONAL EN EL INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA. Estatuto publicado en la Primera Sección del Diario Oficial de la Federación, el miércoles 24 de junio de 2009.

ESTATUTO ORGÁNICO DE AEROPUERTOS Y SERVICIOS AUXILIARES. Estatuto publicado en la Segunda Sección del Diario Oficial de la Federación, el miércoles 20 de octubre de 2004.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 18 DE NOVIEMBRE DE 2005.

ESTATUTO ORGÁNICO DE LA COMISIÓN NACIONAL DE CULTURA FÍSICA Y DEPORTE. Estatuto publicado en el Diario Oficial de la Federación, el lunes 20 de octubre de 2003.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 30 DE OCTUBRE DE 2007.

ESTATUTO ORGÁNICO DE LA COMISIÓN NACIONAL FORESTAL. Estatuto publicado en la Primera Sección del Diario Oficial de la Federación, el lunes 7 de agosto de 2006.
ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 27 DE SEPTIEMBRE DE 2010.

ESTATUTO ORGÁNICO DE LA PROCURADURÍA FEDERAL DEL CONSUMIDOR. Estatuto publicado en la Primera Sección del Diario Oficial de la Federación, el lunes 10 de julio de 2006.
ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 21 DE JULIO DE 2010.

LEY DE COORDINACIÓN FISCAL. Ley publicada en el Diario Oficial de la Federación, el miércoles 27 de diciembre de 1978.
ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 24 DE JUNIO DE 2009.

LEY DE EDUCACIÓN DEL DISTRITO FEDERAL. Ley publicada en la Gaceta Oficial del Distrito Federal, el jueves 8 de junio de 2000.
ÚLTIMA REFORMA PUBLICADA EN LA GACETA OFICIAL DEL DISTRITO FEDERAL: 3 DE FEBRERO DE 2011.

LEY DE FISCALIZACIÓN Y RENDICIÓN DE CUENTAS DE LA FEDERACIÓN. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el viernes 29 de mayo de 2009.
ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 18 DE JUNIO DE 2010.

LEY DE INSTITUCIONES DE CRÉDITO. Ley publicada en el Diario Oficial de la Federación, el miércoles 18 de julio de 1990.
ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 25 DE MAYO DE 2010.

LEY DE OBRAS PUBLICAS Y SERVICIOS RELACIONADOS CON LAS MISMAS. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el martes 4 de enero de 2000.
ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 28 DE MAYO DE 2009.

LEY DE PETRÓLEOS MEXICANOS. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el viernes 28 de noviembre de 2008.

LEY DEL IMPUESTO AL VALOR AGREGADO. Ley publicada en el Diario Oficial de la Federación, el viernes 29 de diciembre de 1978.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 27 DE ABRIL DE 2010.

ÚLTIMA MODIFICACION MISCELANEA FISCAL PUBLICADA EN DIARIO OFICIAL DE LA FEDERACION: 20 DE ENERO DE 2003.

LEY DEL IMPUESTO EMPRESARIAL A TASA ÚNICA. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el lunes 1 de octubre de 2007.

LEY DEL IMPUESTO SOBRE LA RENTA. Ley publicada en el Diario Oficial de la Federación, el Martes 30 de Diciembre de 1980.

LEY DEL MERCADO DE VALORES. Ley publicada en la Cuarta Sección del Diario Oficial de la Federación, el viernes 30 de diciembre de 2005.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 6 DE MAYO DE 2009.

LEY DEL REGISTRO PÚBLICO VEHICULAR. Ley publicada en la Sección Primera del Diario Oficial de la Federación, el miércoles 1º de septiembre de 2004.

LEY DEL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA. Ley publicada en la Segunda Sección del Diario Oficial de la Federación, el viernes 15 de diciembre de 1995.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 6 DE MAYO DE 2009.

LEY DEL SERVICIO DE TESORERÍA DE LA FEDERACIÓN. Ley publicada en la Segunda Sección del Diario Oficial de la Federación, el martes 31 de diciembre de 1985.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 1 DE OCTUBRE DE 2007.

LEY DE LA POLICÍA FEDERAL. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el lunes 1 de junio de 2009.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 30 DE NOVIEMBRE DE 2010.

LEY FEDERAL DE EXTINCIÓN DE DOMINIO, REGLAMENTARIA DEL ARTICULO 22 DE LA CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el viernes 29 de mayo de 2009.

LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el jueves 4 de agosto de 1994.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 30 DE MAYO DE 2000.

LEY FEDERAL DE PROCEDIMIENTO CONTENCIOSO ADMINISTRATIVO. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el jueves 1 de diciembre de 2005.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 28 DE ENERO DE 2011.

LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR. Ley publicada en el Diario Oficial de la Federación, el jueves 24 de diciembre de 1992.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 28 DE ENERO DE 2011.

LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el martes 11 de junio de 2002.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 5 DE JULIO DE 2010.

LEY FEDERAL PARA LA ADMINISTRACIÓN Y ENAJENACIÓN DE BIENES DEL SECTOR PÚBLICO. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el jueves 19 de diciembre de 2002.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACION: 23 DE FEBRERO DE 2005.

LEY GENERAL DE BIENES NACIONALES. Ley publicada la Primera Sección del Diario Oficial de la Federación, el jueves 20 de mayo de 2004.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 31 DE AGOSTO DE 2007.

LEY GENERAL DE ORGANIZACIONES Y ACTIVIDADES AUXILIARES DEL CRÉDITO. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el lunes 14 de enero de 1985.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 20 DE AGOSTO DE 2008.

LEY GENERAL DE TÍTULOS Y OPERACIONES DE CRÉDITO. Ley publicada en el Diario Oficial de la Federación, el sábado 27 de agosto de 1932.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 20 DE AGOSTO DE 2008.

LEY MODELO DE LA CNUDMI SOBRE COMERCIO ELECTRÓNICO.

Aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, el 12 de junio de 1996.

LEY MODELO DE LA CNUDMI SOBRE LAS FIRMAS ELECTRÓNICAS.

Aprobada por la Comisión de Naciones Unidas para el Derecho Mercantil Internacional, el 5 de julio de 2001.

LEY N° 527. Decretada por el Congreso de Colombia, en 1999.

LEY ORGÁNICA DEL PODER JUDICIAL DE LA FEDERACIÓN. Ley publicada en el Diario Oficial de la Federación, el viernes 26 de mayo de 1995.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 30 DE NOVIEMBRE DE 2010.

LEY PARA LA TRANSPARENCIA Y ORDENAMIENTO DE LOS SERVICIOS FINANCIEROS. Ley publicada en la Primera Sección del Diario Oficial de la Federación, el viernes 15 de junio de 2007.

ÚLTIMA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN: 25 DE MAYO DE 2010.

LEY PARA PREVENIR Y ERRADICAR LA TRATA DE PERSONAS, EL ABUSO SEXUAL Y LA EXPLOTACIÓN SEXUAL COMERCIAL INFANTIL PARA EL DISTRITO FEDERAL. Ley publicada en la Gaceta Oficial del Distrito Federal, el viernes 24 de octubre de 2008.

REGLAMENTO DEL CÓDIGO DE COMERCIO EN MATERIA DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN. Reglamento publicado en la Sección Segunda del Diario Oficial de la Federación, el lunes 19 de julio de 2004.

PÁGINAS WEB

<http://español.regions.com>

www.abm.org.mx

www.aecem.org

www.banorte.com

www.blog.banregio.com

www.cmt.es

www.ebanking.cl

www.enbfl.com

www.federalreserve.gov

www.inapam.gob.mx

www.ine.es

www.inegi.org.mx

www.mincomercio.gov.co

www.nafcu.com

www.ocde.com

www.uncitral.org

www.uncitral.org

www.wachovia.com