

Universidad de Valparaíso. Chile.

Facultad de Ciencias Jurídicas y Sociales.

Escuela de Derecho.

Aspectos Jurídicos del Comercio Electrónico

realizado mediante la Internet.

Claudia Loreto Bardi Álvarez.

Valparaíso, Junio 2003.

Agradecimientos.

A mis padres, Amanda y Luis, por su cariño y comprensión;

A mi marido Juan Pablo, por su apoyo incondicional; y

A todos los que de alguna manera colaboraron en la realización de esta memoria.

ÍNDICE.

Introducción.

1. Planteamiento.	10
2. Método, estructura y fuentes.	11
3. Objetivos del trabajo.	13
4. Nociones generales.	13
4.1. La Internet.	13
4.1.1. Breve historia.	14
4.1.2. Concepto.	15
4.1.3. La Internet y las otras redes de telecomunicaciones.	16
4.1.4. El Ciberespacio y la Aldea Global.	17
4.2. El Comercio Electrónico.	18
4.2.1. El Mercado Electrónico y su relación con el Comercio Electrónico.	18
4.2.2. Concepto.	19
4.2.3. Contenido.	20
4.2.4. Origen y evolución.	21
4.2.5. Categorías.	21
4.2.5.1. Comercio Electrónico empresa-empresa.	21
4.2.5.2. Comercio Electrónico empresa-consumidor.	22
4.2.6. Clasificaciones.	22
4.2.7. Similitudes entre el comercio electrónico y el comercio físico o tradicional... ..	23
4.2.8. Manifestaciones del Comercio Electrónico.	24
4.2.8.1. El correo electrónico.	24
4.2.8.2. La WWW.	25
4.2.8.3. El sistema EDI.	25
4.2.8.3.1. Concepto y requisitos.	25
4.2.8.3.2. Funcionamiento del EDI.	26
4.2.8.3.3. Elementos del EDI.	26
4.2.8.3.4. EDI, un tipo de contratación electrónica.	28
4.2.8.3.5. La normalización y la estructuración de los datos.	28
4.2.8.3.6. Beneficios del sistema EDI.	30

Capítulo I.

Los Contratos Electrónicos o Digitales.

1. Generalidades.	32
2. Concepto.	33
3. Distinción previa.	34
4. Elementos de los contratos electrónicos.	34
4.1. La Voluntad.	35
4.1.1. La voluntad, base del contrato.	35
4.1.2. La adhesión.	37
4.1.3. Oferta y aceptación.	39
4.1.3.1. La oferta o policitud electrónica.	39
4.1.3.2. La aceptación electrónica.	41
4.1.4. Momento de formación del consentimiento.	44
4.1.5. Lugar de formación del consentimiento.	48
4.1.6. El consentimiento en los contratos reales y solemnes.	50
4.1.7. Vicios del consentimiento.	52
4.1.7.1. Error.	52
4.1.7.2. Fuerza.	53
4.1.7.3. Dolo.	54
4.2. Capacidad.	55
4.3. Objeto.	56
4.4. Causa.	57
4.5. Formalidades.	57
4.5.1. Posibilidad de dar cumplimiento a las formalidades del Derecho Civil a través de medios electrónicos.	58
4.5.2. Requisito de escriturar.	61
4.5.3. La firma.	62
5. Fases de la contratación electrónica.	63
5.1. Fase de generación o precontrato.	63
5.2. Fase de perfeccionamiento.	64

5.3. Conclusión o pago.	65
5.3.1. Forma de dar cumplimiento a las obligaciones.	65
5.3.2. El dinero electrónico o virtual.	66
5.3.3. Las Transferencias Electrónicas de Fondos (T.E.F.).	66
5.3.3.1. Concepto.	66
5.3.3.2. Formas que pueden revestir las T.E.F.	67
6. La interpretación contractual.	73
6.1. La interpretación en el Código Civil.	73
6.2. Variaciones en la interpretación de los contratos.	74
7. Los riesgos en la contratación digital.	75
8. Problemas de Derecho Internacional Privado relacionados con los Contratos Electrónicos.	78
8.1. Contratos celebrados en Chile.	79
8.2. Contratos celebrados en el extranjero.	79
8.3. Competencia jurisdiccional.	82
8.4. Posible solución.	83
8.4.1. Convenios Internacionales aplicables al contrato celebrado mediante la Internet.	84
8.4.2. La opinión de los Organismos Internacionales.	86

Capítulo II.

El Documento Electrónico.

1. Generalidades.	89
2. El documento en sentido genérico.	90
2.1. Concepto.	90
2.2. Documento e instrumento.	91
2.3. Clasificación.	92
2.4. Estructura del documento.	93
2.4.1. Elemento material.	93
2.4.2. Elemento intelectual, ideológico o docente.	94
3. El documento emitido por medios electrónicos.	95

3.1. Concepto.	95
3.2. Concepto legal de documento electrónico.	96
3.3. Clasificaciones.	97
3.4. Composición del documento electrónico atendidos los requisitos del documento tradicional.	100
3.4.1. Elemento material del documento electrónico.	100
3.4.2. Elemento intelectual del documento electrónico.	101
3.5. Naturaleza jurídica del documento electrónico.	101
3.6. El lenguaje del documento electrónico.	102
3.6.1. Código Binario.	103
3.6.2. Lenguajes de interpretación.	103
3.6.3. Etapas en la comunicación hombre-computador.	104
3.7. El documento electrónico de la Administración Pública.	104
3.7.1. La Ley 19.799 en relación con el documento electrónico de los Órganos del Estado.	106
3.7.2. Leyes especiales.	106
4. Documentos privados y públicos electrónicos.	106
4.1. Requisitos propios del documento electrónico.	106
4.2. El documento electrónico como instrumento público.....	107
• Requisitos del Instrumento Público Electrónico.	109
5. Valor probatorio del documento electrónico.	111
5.1. Criterios de apreciación de la prueba.	111
5.2. Admisibilidad y valor probatorio del documento electrónico en el derecho chileno.	112
5.2.1. Ley 19.799 y el valor probatorio del documento electrónico.	113
5.2.2. Reconocimiento legal del los documentos electrónicos en otras disposiciones nacionales.	114
5.3. Admisibilidad y eficacia probatoria del documento electrónico en el derecho comparado.	119
5.3.1. España.	120
5.3.2. Italia.	122
5.3.3. Francia.	124
5.3.4. Estados Unidos.	126
5.3.5. Inglaterra.	128

5.4. La opinión de los Organismos Internacionales.	129
5.4.1. Recomendación de Naciones Unidas sobre el valor legal de los registros computacionales (1985).	129
5.4.2. Ley Modelo de UNCITRAL sobre Comercio Electrónico.	130

Capítulo III.

Seguridad de las Transacciones Mercantiles Electrónicas.

1. Nociones básicas.	131
2. Problemas y principio relativos a la seguridad de los mensajes electrónicos.	132
3. La encriptación.	133
3.1. Concepto.	133
3.2. Sistemas criptográficos en general.	134
3.2.1. Métodos de criptografía simétrica o de clave única.	134
3.2.2. Métodos de criptografía asimétrica o de clave doble.	135
3.2.3. Otras variantes.	137
3.2.3.1. Métodos híbridos.	137
3.2.3.2. Método asimétrico con utilización de Código Hash. Firma digital.	137
4. La Firma Electrónica.	139
4.1. Nociones básicas.	139
4.2. Concepto.	140
4.3. Ventajas de la firma electrónica.	141
4.4. Equivalencia funcional entre la firma digital y la firma manuscrita.	141
4.5. Sistemas de encriptación utilizados en la firma digital.	142
4.6. La firma electrónica en la legislación chilena.	143
4.6.1. Concepto legal de firma electrónica.	143
4.6.2. Distinción. La firma electrónica avanzada.	143
5. Los Certificados Digitales.	144
5.1. Planteamiento.	144
5.2. Conceptos y clases de certificados.	145
5.3. Elementos personales de los certificados.	147
5.3.1. Autoridad de certificación.	147

5.3.2. Suscriptor del certificado.	148
5.3.2.1. Naturaleza del suscriptor del certificado.	148
5.3.2.2. Relación del suscriptor del certificado con la entidad certificadora.	151
5.3.3. Tercero, usuario del certificado.	151
5.4. Los certificados digitales en la legislación chilena.	152
5.4.1. Regulación, denominación y concepto de los certificados.	152
5.4.2. Contenido de los certificados.	153
5.4.3. Vigencia del certificado.	153
5.4.3.1. Vigencia temporal.	153
5.4.3.2. Vigencia territorial.	155
6. Los Prestadores de Servicios de Certificación.	156
6.1. Distinción doctrinal. La tercera parte de confianza.	156
6.2. Concepto y terminología.	157
6.3. Naturaleza jurídica.	157
6.4. Los prestadores de servicios de certificación en la legislación chilena.	159
6.4.1. Regulación.	159
6.4.2. Concepto.	159
6.4.3. Clasificación de los prestadores de servicios de certificación.	160
6.4.3.1. Prestador de servicios de certificación domiciliado y no domiciliado en Chile.	160
6.4.3.2. Prestador de servicios de certificación acreditado y no acreditado.	161
6.4.4. Obligaciones de los prestadores de servicios de certificación.	162
6.4.4.1. Obligaciones comunes a todo prestador de servicios de certificación.	162
6.4.4.2. Obligaciones propias de los prestadores de servicios de certificación acreditados.	163
6.4.5. Responsabilidad civil de los prestadores de servicios de certificación.	165
6.4.6. Acreditación de los prestadores de servicios de certificación.	167
6.4.6.1. Concepto.	167
6.4.6.2. Importancia de la acreditación.	167
6.4.6.3. Requisitos del prestador de servicios de certificación para ser acreditado.	168
6.4.6.4. Procedimiento de acreditación.	168
6.4.6.5. Efectos de la acreditación.	170
6.4.6.6. Cesación de la acreditación y cancelación de la inscripción.	170

6.4.6.7. Facultad Inspector de la Entidad Acreditadora.	172
6.4.6.8. Registro Público de prestadores de servicios de certificación acreditados...	173
7. Regulación relativa a la Seguridad del Comercio Electrónico.	173
7.1. La Ley chilena.	174
7.1.1. La Ley 19.799 y el Reglamento.	174
7.1.2. Otras disposiciones nacionales.	174
7.1.2.1. Normativa aduanera.	174
7.1.2.2. Normativa tributaria.	176
7.2. Derecho comparado.	177
7.2.1. Ley de Utah de 1995.	178
7.2.2. Ley alemana.	178
7.3. Regulación internacional.	180
7.3.1. Ley Modelo sobre Comercio Electrónico de UNCITRAL.	180
7.3.2. Directiva Europea 93/1999 sobre Firma Digital.	181
Conclusiones.	183
Bibliografía.	188
Anexo.	200

INTRODUCCIÓN.

1. Planteamiento.

El progreso tecnológico de los últimos años ha producido cambios sustanciales en casi todos los aspectos de la vida del hombre. Ello ha llevado a algunos autores a plantear que la humanidad se enfrenta a una verdadera revolución social, cultural, económica y política de insospechables repercusiones.

Se trata, principalmente, de los avances en el área de la *informática*¹ y de la *telemática*², como los computadores, las telecomunicaciones y los programas informáticos, los que utilizados de manera combinada, han permitido el nacimiento de la *Internet*.

Esta Red abierta que conecta a millones de ordenadores en el mundo, ha generado un explosivo crecimiento del *Comercio Electrónico*, transformándolo en un medio de intercambio de productos atractivo tanto para empresarios como para consumidores finales. Sus ventajas están a la vista: mejora la competitividad, reduce costos y otorga mayor celeridad en el desarrollo de las relaciones mercantiles. A través de éste, las personas tienen acceso a una gran variedad de bienes, lo que incrementa sus posibilidades de elección. Desde otra perspectiva, crea nuevas oportunidades de empleo y transforma los medios de pago tradicionales. En resumen, modifica la forma tradicional de concebir el mercado, y en consecuencia la de hacer negocios.

Todo esto se manifiesta en la aparición de numerosas tiendas virtuales, donde es posible adquirir una gran cantidad de productos, en los proyectos de teletrabajo, en las relaciones entre proveedores y empresas a través del EDI, en los sistemas de pago electrónico, etc.

¹ La *informática* es “la ciencia del tratamiento automatizado o electrónico de la información”. Jijena Leiva, Renato Javier, “Comercio electrónico y derecho. La problemática jurídica del Comercio Electrónico”, *REDI: Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., N° 9, Abril 1999 (c 1997-2002, vLex Networks). Sitio Web vlex.com, España (http://v2.vlex.com/global/redi/redi_numero.asp?numero=%239&fecha=Abril+1999), http://v2.vlex.com/es/ppv/doctrina/fuente_29_numero_%239 , apartado I, Introducción.

² La palabra *telemática* surge de la unión de “telecomunicaciones-informática”. Es la informática aplicada a las telecomunicaciones, por lo que se relaciona con las redes digitales. Jijena Leiva, Renato Javier, “Comercio electrónico y derecho. La problemática jurídica del Comercio Electrónico”, op. cit., apartado I, Introducción.

Pero el comercio electrónico realizado a través de Internet no sólo ha transformado las actividades cotidianas del hombre y el modo de operar del mercado. Sus efectos han llegado al funcionamiento de la sociedad misma.

Esto debido a que posibilita el intercambio entre individuos y sociedades ubicadas a miles de kilómetros de distancia, en forma instantánea, generando dependencia, e incluso, en cierto sentido, eliminando las fronteras geográficas.

De este nuevo escenario, surgen una serie de problemáticas que el derecho debe resolver. El sistema jurídico debe permitir el uso de las nuevas tecnologías en el ámbito del comercio, además de dar confianza a los usuarios.

Esta confianza sólo se alcanza con un marco regulatorio claro para el comercio electrónico, el que debe incluir a los *contratos celebrados por medios electrónicos de comunicación* y al *documento electrónico*. Ambos requieren el mismo reconocimiento y protección legal que los realizados tradicionalmente en soporte de papel.

El *tema de la seguridad* también cobra relevancia en el desarrollo de la confianza, debido a que en principio, el medio por donde transita la información es inseguro. Por esto, tales actos y documentos celebrados mediante la Internet requieren de protección, la que se obtiene a través de los diversos sistemas de seguridad ideados por la tecnología.

2. Método, estructura y fuentes.

Utilizando un sistema esencialmente *descriptivo*, el presente trabajo se inicia con el tratamiento de la Internet y el Comercio Electrónico. Esta parte introductoria general, pretende ilustrar y ubicar al lector, además de dilucidar algunas dudas conceptuales, propias de los temas relativamente nuevos.

Luego, en los diferentes capítulos, se distinguen tres de las principales *problemáticas jurídicas del Comercio Electrónico*.³

En el Capítulo I se tratan los *Contratos Electrónicos*, los que adquieren ciertos matices que los diferencian de los tradicionales del Derecho Civil.

³ No es posible dejar de reconocer la existencia de otras problemáticas relativas al comercio electrónico, las que exceden el ámbito estrictamente mercantil, como la privacidad de los datos que circulan por la red y la protección de la propiedad intelectual e industrial de los bienes electrónicos.

Por ello, cobran significación sus diversos elementos, particularmente la voluntad (el momento y lugar de formación del consentimiento) y las formalidades.

Este capítulo también se refiere a las fases de la contratación electrónica, a la interpretación y a los riesgos de esta clase de contratos.

Al final, se abordan los problemas de derecho internacional privado que pueden originar los contratos electrónicos, en caso que involucren a agentes de procedencia y características diversas.

El Capítulo II está dedicado al *Documento Electrónico*, el que tiene importancia debido a que la posibilidad de garantizar su cumplimiento por la vía judicial depende del reconocimiento que el derecho haga de su existencia.

Este capítulo comienza explicando el documento en un sentido genérico, para luego, y sobre la base de tal explicación, avocarse al documento emitido electrónicamente, incluyendo su versión pública y privada.

Especial interés tiene el tema de la prueba del documento electrónico, el que es analizado desde el punto de vista del derecho chileno, del derecho comparado y del derecho internacional.

Por último, el Capítulo III se refiere a la *Seguridad de las transacciones mercantiles electrónicas*, debido a que los contratos y documentos utilizados en las operaciones comerciales y que “viajan” a través de redes públicas como Internet, requieren de sistemas que garanticen su integridad, autenticidad y confidencialidad.

Por esto, el capítulo tercero trata los diversos métodos de encriptación de la información, en especial los asimétricos o de doble clave. Luego se dedica a la firma electrónica, a los certificados digitales y a los prestadores de servicios de certificación.

Con el objeto de estudiar cada una de estas problemáticas, se recurrió tanto a la doctrina nacional como extranjera. Sin embargo, por tratarse de un tema relativamente novedoso, se pudo constatar que los diversos autores difieren en muchos de los aspectos relacionados con el comercio electrónico, incluidos sus conceptos fundamentales.

También, se invocó la legislación chilena, como la Ley 19.799 y su Reglamento, además de otras normas que de alguna manera hacen referencia o tienen relación con el Comercio Electrónico.

Se recurrió, además, al derecho comparado, con el propósito de conocer otras respuestas legislativas a los problemas del comercio electrónico.

Por último, y por tratarse de un tema que puede involucrar intereses de distintos estados, se apeló al derecho internacional, principalmente a la *Ley Modelo sobre*

Comercio Electrónico, aprobada en 1996 por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) y a algunas directivas europeas.

3. Objetivos del trabajo.

Como lo indican las cifras, los montos involucrados en las operaciones de Comercio Electrónico realizadas mediante la Internet son cada vez mayores. Sin embargo, este crecimiento podría aumentar, si se otorgara mayor certeza y seguridad jurídica a los usuarios.

Por esto, es importante determinar y analizar los principales conflictos jurídicos que origina esta forma de comercio, para así proponer algunas vías de solución, fundadas en la doctrina y en la legislación vigente.

La difusión del tema entre los estudiosos del derecho resulta trascendental, ya que cada vez más se incrementa el número de conflictos derivados de actuaciones a través de la red.

4. Nociones generales.

El presente trabajo se centra en el estudio del Comercio Electrónico, particularmente en el realizado vía Internet. Ello sin perjuicio de reconocer que anteriores innovaciones, como el teléfono y el fax, se utilizan de manera similar, aunque más limitada, para realizar operaciones mercantiles digitales.

Como ha sido la Internet la que ha llevado al Comercio Electrónico al sitio que ocupa en la actualidad, parece fundamental conocer sus orígenes y su relación con las otras redes de comunicación.

4.1. La Internet.

El crecimiento de la Internet ha alcanzado niveles difíciles de comparar. La radio, por ejemplo, tardó casi cuarenta años en llegar a una audiencia de cincuenta millones de

personas. La televisión demoró trece. “*La Red*”, en menos de cuatro años sobrepasó esa cantidad. Es más, según algunos entendidos, se espera para el año 2005, que un billón de personas la utilice.⁴

4.1.1. Breve historia.

En 1957, durante la Guerra Fría, el presidente norteamericano Dwight Eisenhower ordenó la creación de la Agencia de Proyectos Avanzados de Investigación (ARPA).⁵

Posteriormente, en 1962, J.C.R. Licklider, un psicólogo e informático, propuso el establecimiento de una red de computadores para permitir la comunicación entre los científicos de ARPA.

Sin embargo, no fue hasta fines de los años sesenta cuando este proyecto se concretó. Con el objeto de evitar un centro neurálgico de comunicaciones que pudiera ser destruido por un eventual ataque nuclear, las fuerzas armadas norteamericanas dispusieron la creación de una red nacional interconectada. Dicha red, debía ser capaz de reestablecerse, evitando un posible bloqueo de las comunicaciones. Este proyecto se llamo ARPANET.⁶

Durante los años setenta ARPANET dejó de ser un proyecto exclusivamente militar. Las instituciones académicas se interesaron por esta forma de conexión, por lo que diferentes grupos de científicos la utilizaron para el intercambio de información de distinto tipo.

El acceso de civiles llevó a que el área de defensa de Estados Unidos creara una nueva red militar clasificada, llamada MILNET. Paralelamente, la National Science Foundation creó la NSFNET, que en 1974 enlazaba a ciento veinte universidades.

Durante los siguientes años nacieron una serie de redes diferentes alrededor del mundo. Sin embargo, no podían comunicarse entre ellas ya que utilizaban diferentes protocolos o estándares para la transmisión de datos.

⁴ Otero Alvarado, Jorge y Lanckenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, Estudio Jurídico Otero, ENTEL Internet, Santiago, Chile, 1999, pág. 10.

⁵ *Advanced Research Projects Agency*.

⁶ *Advanced Research Projects Agency Network*.

En 1981 se terminó de definir el protocolo TCP/IP (*Transfer Control Protocol / Internet Protocol*)⁷, el que fue adoptado por ARPANET como estándar en 1982. La implementación del TCP/IP permitió a las diversas redes conectarse en una verdadera red de redes: la Internet.

En 1983 ARPANET se separó de la red militar que la originó, lo que puede considerarse como el nacimiento de Internet. Así, se deja abierto el paso para que todas las empresas, universidades y demás instituciones accedan a la red.

Más tarde, en 1989, el informático Timothy Berners-Lee desarrolló la “World Wide Web” o “WWW” que facilitó la manera de interactuar y encontrar datos en Internet.⁸

La creación de la WWW, unida a la proliferación de los computadores personales llevó a un crecimiento de Internet en el mundo.

Como consecuencia de lo anterior, en 1995 se produjo una verdadera explosión en el área comercial. Se desarrolló de manera definitiva el comercio electrónico, para la compra de bienes y servicios a través de la Red.

En Chile, el comercio electrónico empezó en los primeros meses de 1998, con algunas pequeñas tiendas virtuales, y con la participación de grandes casas comerciales.⁹

4.1.2. Concepto.

La palabra Internet proviene de la abreviatura de *Interconnected Networks*, es decir, redes interconectadas. De este modo, siguiendo su derivación etimológica, ésta designa en forma genérica a todas las redes digitales entrelazadas.

⁷ El “TCP” y el “IP” son definidos como la nueva norma para la transferencia de información entre los equipos, ya que pueden correr en una amplia variedad de software. Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, Chile 2000, pp. 105. Tesis (Licenciatura en Derecho), Facultad de Ciencias Jurídicas y Sociales, Escuela de Derecho Universidad Central de Chile, pág. 6.

⁸ La novedad del sistema WWW se debe a que integra en una sola interfaz los diferentes servicios utilizados en las distintas redes, como el FTP (que es aquel que permite transferir archivos entre computadores conectados a Internet), el servicio de noticias, el de correo electrónico, y el denominado Gopher (que organiza la información y permite acceder a ella de manera más sencilla). Pero además, funciona sobre la base de un sistema denominado http o formato de hipertexto, lo que le permite utilizar documentos con imágenes, audio y video. Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit. , pág. 10.

⁹ Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, op.cit., pág. 7.

Sin embargo, mayoritariamente, “Internet” es el nombre que recibe *la red pública*¹⁰ más importante que existe en la actualidad. La también denominada “Red de redes.”

La Internet está formada por millones de computadores conectados en el mundo (llamados servidores) los que se encuentran entrelazados entre sí a través de distintos mecanismos, como la fibra óptica, los satélites y las líneas telefónicas.

Generalmente, las personas acceden a la Internet por medio de computadores personales, teléfonos móviles o agendas digitales, a los que se incorpora un aparato denominado *modem*, que se conecta a la línea telefónica o a las diversas tecnologías de banda ancha.¹¹

4.1.3. La Internet y las otras redes de telecomunicaciones.

La información en las operaciones de comercio electrónico puede ser transmitida mediante redes digitales cerradas o abiertas.

Las *redes cerradas* son de propiedad y administradas por entes específicos, y no admiten el ingreso de terceros sin autorización. Éstas posibilitan un mayor grado de seguridad.

Entre las redes cerradas es posible distinguir:

1) Redes de Valor Agregado.¹²

Estas son redes de transmisión de datos creadas por particulares, los que contratan a terceros que prestan servicios al grupo de abonados.

Generalmente funcionan en sectores específicos de la producción y el comercio. Así por ejemplo, existe ODETTE para la industria automotriz, EDIFICE, para el ámbito electrónico, y RINET para el grupo bancario.¹³

Este sistema, facilita el acceso a la red, brinda asesoría y otorga una extensa variedad de servicios a sus usuarios. Además da seguridad al contenido y transmisión de datos. Sin embargo, tiene el inconveniente de que su costo es bastante elevado.¹⁴

¹⁰ Como se verá (apartado 4.1.3. de la Introducción), las redes digitales pueden ser públicas o privadas dependiendo de si el acceso a ellas es libre o no para todas las personas.

¹¹ En la actualidad, el uso de estas líneas está dando paso al empleo de la fibra óptica y a las transmisiones inalámbricas de datos (o “*wireless*”).

¹² También se denominan VAN (*Value Added Network*).

¹³ En Chile está EasyMail, Editrade y Transbank.

¹⁴ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, Granada, Editorial Comares S.L, 1997, pág. 85.

2) Redes Privadas.

Son aquellas redes de comunicación elaboradas por una determinada empresa o institución y disponible sólo para los usuarios autorizados.

Se utilizan en grandes industrias e instituciones por la seguridad y confidencialidad que otorgan al intercambio de información.

Las *redes abiertas o públicas* son aquellas en que nadie puede ser impedido de acceder y operar. La más grande es Internet.

Uno de los mayores problemas del comercio electrónico realizado mediante redes públicas radica en la inseguridad de los datos transmitidos entre los usuarios. Por esto, surgen diversos sistemas para garantizar la seguridad de las operaciones, como la firma electrónica, los certificados digitales y los proveedores de servicios de certificación.¹⁵

4.1.4. El Ciberespacio y la Aldea Global.

La Internet, formada por la interconexión de ordenadores y servidores, crea el denominado *Ciberespacio (Cyberspace)*.¹⁶

Este concepto se utiliza para denominar aquel espacio físicamente intangible donde existe Internet, es decir, el lugar por donde viajan los mensajes de datos y ocurren las transacciones electrónicas.¹⁷

Es justamente en este sitio donde se genera la llamada *Aldea Global*.

Internet crea una nueva comunidad que parece no tener fronteras geográficamente delimitadas. De esta manera, nace un nuevo mundo creado por las conexiones de los computadores, donde cada terminal es parte integrante de esta aldea o comunidad.¹⁸

Ejemplo de ella es la publicación de libros prohibidos por la justicia chilena, de la misma manera como sucedió con la divulgación de la vida del ex presidente francés Francois Mitterand, a través de una página en Internet. La prohibición de la justicia gala

¹⁵ Cfr. Capítulo III de este trabajo.

¹⁶ Palabra acuñada en 1984 por William Gibson en la novela *Neuromancer* (Berkley Publishing Group, New York), Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, Primera Edición, Barcelona, Editorial Bosch S.A., Abril 2000, pág. 121.

¹⁷ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit., pág. 10.

¹⁸ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op. cit., pág. 10.

no pudo evitar que los franceses accedieran a la historia escrita por el médico personal del político. Las acciones legales no fueron acogidas debido a que el proveedor de servicios de Internet estaba ubicado fuera del territorio de la república francesa.¹⁹

Este nuevo escenario plantea diversos problemas, como la determinación del tribunal competente para conocer de los conflictos, la legislación aplicable, y el lugar, forma y oportunidad en que se perfeccionan las transacciones electrónicas.²⁰

4.2. El Comercio Electrónico.

A través de la Internet las personas se comunican y buscan información, pero además realizan transacciones.

Tales operaciones efectuadas mediante la Red, se constituyen hoy en la forma más importante de *Comercio Electrónico*.

4.2.1. El Mercado Electrónico y su relación con el Comercio Electrónico.

El *Mercado Electrónico* es aquel donde los productores, proveedores, intermediarios y consumidores interactúan digitalmente de alguna manera. Es una representación virtual del mercado físico o tradicional, debido a que es el sitio donde los productos, sean bienes o servicios, son comercializados.

En consecuencia, el *Comercio Electrónico*, tiene lugar en el Mercado Electrónico.

La infraestructura física de este mercado, y por consiguiente, la del comercio electrónico, está constituida por las *redes de telecomunicaciones*, como las de telefonía, ópticas, inalámbricas y cualquier otra que otorgue servicios de comunicación. También por los *aparatos y herramientas que permiten acceder a dichas redes*, como los computadores o los teléfonos móviles (incluidos el hardware y el software). Y por

¹⁹ Ramos Suárez, Fernando, “Problemas jurídicos del Comercio Electrónico”, REDI: *Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., N° 2, Septiembre 1998 (c 1997-2002, vLex Networks). Sitio Web vLex, España (http://v2.vlex.com/global/redi/redi_default.asp), http://v2.vlex.com/es/ppv/doctrina/fuente_29_numero_%232 , apartado II, D.

²⁰ Cfr. Capítulo I, apartado 8 de esta memoria.

último, por *otras aplicaciones y servicios de apoyo*, como los sistemas para efectuar pagos electrónicamente.²¹

4.2.2. Concepto.

Por tratarse de un fenómeno relativamente nuevo, el *Comercio Electrónico o Digital*²² ha sido objeto de diversas definiciones. Entre ellas se destacarán tres.

Así, en primer lugar, se ha dicho que el comercio electrónico es *todo intercambio de datos por medios electrónicos, relacionado o no con la actividad comercial en sentido estricto*.²³

Tal concepto resulta demasiado amplio a los ojos de este estudio, en el que sólo se incluyen los actos relativos al ámbito mercantil.²⁴

Restringido a actos comerciales, también se ha definido como el vasto conjunto de actividades *con finalidad mercantil* que se desarrolla mediante el uso de sistemas de procesamiento de datos y de comunicaciones, sin que exista un contacto físico directo entre quien oferta un bien o un servicio y quien lo demanda. Se incluye no sólo los actos comerciales directos, como la compraventa o el arriendo, sino también las acciones preparatorias o conexas como las de publicidad o mercadeo.²⁵

²¹ Otero Alvarado, Jorge y Lanckenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op. cit., pág. 13.

²² Existen autores que consideran inadecuado el nombre “comercio electrónico”, porque habría muy poco de electrónico en él. Plantean que la designación correcta sería *comercio digital*, debido a que es “la transformación de transacciones y procesos basados en papel en procesos digitales (,) en los que la palabra impresa en papel es sustituida por los unos y ceros del código binario.” Cfr. con Masse, David G., “Economic modelling and risk management in public key infrastructures. The business case for a broadly-based highly scalable public key infrastructure.” Versión 3.0, April 15, 1999, pág 2, <http://Chait-Amyyot.ca>, citado por Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, Primera Edición, Madrid, Editorial Civitas, 1998, pág. 26. Sin embargo, a pesar de que se trata de información digital, ésta es transmitida por medios electrónicos, por lo que ambas designaciones son admisibles. Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 26.

²³ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 25.

²⁴ Esto “sin perjuicio de que los problemas planteados por toda comunicación electrónica de datos, sea o no de naturaleza comercial la relación subyacente, sean, básicamente, los mismos, y, por tanto, lo sean también, sustancialmente, las soluciones técnicas y jurídicas aplicables.” Martínez Nadal, Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.26.

²⁵ Millé, Antonio, “Impacto del Comercio Electrónico sobre la Propiedad Intelectual”, Actas del II Congreso Chileno de Derecho Privado, *Revista de Derecho de la Universidad Católica de Valparaíso*, N° XIX, Ediciones Universitarias de Valparaíso, Valparaíso, Chile, 1998, pág. 339

Por último, hay estudiosos para los que el comercio electrónico sólo está constituido por el gran mercado global que representa por definición una actividad generadora de ganancias o pérdidas y *que se realiza a través de la Internet*.²⁶

Esta definición resulta bastante cómoda para efectos de este trabajo. Sin embargo, es demasiado restringida, ya que sólo reconoce a la Internet como forma de comerciar electrónicamente. Como se ha indicado, las operaciones mercantiles electrónicas pueden ser efectuadas utilizando otras redes, e incluso, otros adelantos tecnológicos.

Por esto, para esta memoria, el comercio electrónico debe circunscribirse al ámbito de las *transacciones comerciales digitales*, esto es la compraventa de bienes y la prestación de servicios, así como también, las negociaciones previas y los actos posteriores que tengan relación con dicha transacción (como los pagos electrónicos, por ejemplo) *desarrolladas por medio de las nuevas tecnologías de la comunicaciones*. En consecuencia, la segunda definición parece ser la que mejor se adecua a este estudio.

4.2.3. Contenido.

Como forma de enfrentar los inconvenientes derivados de la multiplicidad de conceptos relativos al comercio electrónico existentes en la doctrina, el profesor Eugenio Gaete²⁷ señala algunos elementos de carácter general, comunes a las diversas definiciones, y que posibilitan plantear su contenido.

Así, menciona como elementos del comercio electrónico:

- 1) El empleo de medios informáticos para la conclusión de los contratos.
- 2) Tanto la oferta como la aceptación, ambas destinadas a producir el acuerdo de voluntades, deben ser realizadas a distancia.
- 3) Debe tratarse de actividades de carácter mercantil, excluyéndose las de otro tipo, como las civiles, laborales, sociales, etc.

²⁶ Gherardelli, Tony, *///C:Netscape/Commer_E.HTM.*, citado por Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 131.

²⁷ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 131.

4.2.4. Origen y evolución.

Los inicios del comercio electrónico se encuentran en el EDI (*Electronic Data Interchange*)²⁸, el que comenzó a ser utilizado hace más de veinte años entre firmas comerciales. Este sistema permitía, a las industrias asociadas, enviar y recibir pedidos, efectuar pagos, obtener información sobre la distribución de productos, etc.

El crecimiento de la Internet y el desarrollo de la WWW, han permitido que, en la actualidad, este tipo de comercio no esté reservado al ámbito empresarial de unos pocos. Hoy se constituye en un aparato gigantesco en el que participan un número cada vez mayor de individuos, incluyendo a empresarios, intermediarios y consumidores finales.

4.2.5. Categorías.

El comercio electrónico, según los agentes implicados, puede dividirse en dos planos diferentes: empresa-empresa y empresa-consumidor.

4.2.5.1. Comercio Electrónico empresa - empresa.²⁹

Se trata del comercio realizado entre industrias, por lo que en la mayoría de los casos se refiere a contactos entre aquéllas que ofrecen productos finales y sus proveedores de insumos.

Para estos efectos, además del EDI, los empresarios utilizan aplicaciones de Internet, como el correo electrónico y la WWW, las que resultan bastante económicas, pero un tanto inseguras.

Esta inseguridad puede determinar la implementación de redes privadas o de valor agregado, con el objeto de garantizar las transacciones. Sin embargo, tales soluciones generalmente son aprovechadas por grandes empresas debido al alto costo que involucran.³⁰

Esta categoría de comercio electrónico suele revestir mayor solidez que el orientado al consumidor, debido a que los involucrados, comúnmente, laboran bajo el principio de

²⁸ También llamado Intercambio Electrónico de Datos. Cfr. Capítulo I, apartado 4.2.8.3. de este trabajo.

²⁹ O *business to business*.

³⁰ Cfr. Capítulo I, apartado 4.1.3. de esta memoria.

la buena fe y la confianza comercial. Esto permite que sus partícipes obtengan información confiable sobre la marcha del mercado, la solvencia de sus proveedores y la rentabilidad de sus inversiones, entre otras materias, lo que posibilita un tipo de comercio fluido y seguro.

Un ejemplo del comercio electrónico entre empresas sería una compañía que utiliza una red para ordenar pedidos a proveedores, recibiendo los cargos y haciendo los pagos, usando o no, el EDI sobre redes particulares o de valor agregado.

4.2.5.2. Comercio Electrónico empresa-consumidor.³¹

Mediante esta clase de comercio electrónico, una empresa ofrece sus productos o servicios a través de la Internet, los que pueden ser adquiridos por un comprador particular. En este caso, el comerciante organiza la información en un *sitio* “donde el consumidor llega para recorrer los escaparates virtuales”.³²

El auge y crecimiento de este tipo de comercio se debe, fundamentalmente, al desarrollo de la Internet como red abierta o pública.

Como ejemplo de esta forma de hacer negocios se pueden mencionar las diversas tiendas sobre Internet (o *virtual malls*) que ofrecen todo tipo de bienes tangibles (como libros, vestuario, flores, etc.) e intangibles (como información textual (diarios, revistas, etc.), imágenes, sonidos y videos) para el consumidor final.

4.2.6. Clasificaciones.

Desde el punto de vista de la forma o medio de distribución de los productos y servicios, es posible distinguir entre comercio electrónico directo y comercio electrónico indirecto.

El *comercio electrónico directo* es aquel en que la transacción completa se realiza a través de una red de telecomunicaciones. De esta forma, el pedido, el pago, e incluso el suministro del bien, pueden efectuarse mediante una red como Internet.

³¹ O *business to consumer*.

³² Millé, Antonio, “Impacto del Comercio Electrónico sobre la Propiedad Intelectual”, op. cit., pág. 341.

Las operaciones de comercio electrónico directo se refieren, en general, a bienes y servicios de carácter inmaterial (también llamados intangibles o blandos), como los softwares, la música y los videos.

El *comercio electrónico indirecto* es aquel en que la transacción consiste en un pedido electrónico de bienes materiales (también denominados tangibles o duros), los que deben ser entregados utilizando los canales tradicionales de distribución, como por ejemplo el correo.

Ejemplo de este tipo de comercio lo constituyen las tiendas virtuales, donde los objetos pueden ser apreciados en una foto o mediante una descripción textual, y una vez adquiridos, se envían al comprador a través de un servicio de correo.

El comercio electrónico también puede ser entendido como *la transacción en línea* o *como el mercado en sí*.

En el primer caso, se refiere a hacer negocios en línea, es decir, a vender y comprar tanto productos como servicios a través de sitios de Internet. Los bienes objeto de estas transacciones pueden ser físicos o digitales, por lo que se incluyen el comercio electrónico directo y el indirecto.

Por otro lado, el *comercio electrónico como el mercado en sí*, es el entorno económico entero que se encuentra en línea, y en el que cualquier comerciante puede localizar proveedores, clientes, inversionistas, agencias gubernamentales e incluso competidores.

4.2.7. Similitudes entre el Comercio Electrónico y el comercio físico o tradicional.

El comercio electrónico es muy parecido al comercio tradicional. Esto debido a que ambos poseen los *mismos elementos y participantes*.

Así, sus elementos comunes son:

- 1) Oferentes o proveedores de bienes o servicios;
- 2) Clientes y consumidores;
- 3) Productos, sean bienes o servicios;
- 4) Metodologías de trabajo, como los procedimientos de promoción, producción, servicios de venta, distribución, etc.

Sin embargo, existe una característica que los diferencia. En el comercio electrónico, *uno de estos elementos (o todos) es (son) sustituido(s) por su homólogo electrónico*. Por ejemplo, puede ser que uno de los participantes sea una empresa que no posee una tienda física, sino que sólo una virtual, por lo que la única forma de acceder a ésta sería a través de la red.

4.2.8. Manifestaciones del Comercio Electrónico.

Por tratarse de una materia en evolución, no existe acuerdo entre los autores sobre las distintas vías a través de las cuales se manifiesta el comercio electrónico.

A pesar de ello, es posible señalar que, en general, se trata de las nuevas tecnologías de la comunicación como son: el correo electrónico, el World Wide Web y el sistema EDI.³³

4.2.8.1. El Correo Electrónico.³⁴

Es una variable electrónica a través de la cual es posible intercambiar información entre diversos computadores, por medio de un intermediario que generalmente es Internet, utilizando códigos alfanuméricos, y traducidos a un texto legible. Tal texto puede ser leído directamente, de la pantalla del computador o de una impresión en una hoja de papel.³⁵

El correo electrónico actúa mediante procesamientos de almacenamiento y reenvío del mensaje, a través de los denominados agentes de transferencia de mensajes.³⁶

³³ Hay estudiosos que agregan el fax y el videotex. Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág.133.

³⁴ También se denomina *mail*.

³⁵ Parisien, Serge & Trudel, Pierre, *Identificación et la certificación dans le commerce électronique*, Editions Ivon Blais Inc., Quebec (1996), citado por Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág.133.

³⁶ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 28.

4.2.8.2. La WWW.

La *World Wide Web*, o simplemente Web, es una aplicación de Internet que juega un importante rol en el comercio electrónico. A diferencia de EDI, facilita las relaciones comerciales ocasionales o a corto plazo, sin necesidad de contratos previos.

Constituye un destacado instrumento de difusión de la información comercial. Pero además, es un medio para realizar transacciones electrónicas, de forma prácticamente interactiva y en línea.³⁷

La información relacionada con el catálogo de bienes y servicios de un proveedor es organizada en un sitio, compuesto generalmente por varias páginas. El individuo interesado en la adquisición accede a ese lugar a través de su conexión a la red.

Si la oferta es de bienes físicos, seleccionando un determinado producto, surge una gran cantidad de información sobre sus características y especificaciones. Para esto, se utilizan incluso imágenes que lo dan a conocer.

Una vez que el interesado manifiesta su voluntad de comprar, se intercambian una serie de mensajes electrónicos que cierran la operación e instrumentan el pago.³⁸

4.2.8.3. El Sistema EDI.

4.2.8.3.1. Concepto y requisitos.

El EDI³⁹ es aquel intercambio electrónico de información estructurada, mediante formatos estandarizados, realizado entre sistemas computacionales.

Las transacciones efectuadas mediante este sistema, requieren de una larga fase de negociación y preparación entre las partes involucradas, con el objeto de establecer los protocolos técnicos y administrativos, así como también los acuerdos que les serán aplicables.⁴⁰

³⁷ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 28.

³⁸ Millé, Antonio, “Impacto del Comercio Electrónico sobre la Propiedad Intelectual”, op. cit., pág. 341.

³⁹ *Electronic Data Interchange* o Intercambio Electrónico de Datos.

⁴⁰ Martínez Nadal, Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.27.

Constituye el origen del comercio electrónico, debido a que comenzó a ser utilizado en la década del setenta entre algunas firmas comerciales.

Tres son los requisitos de este sistema:

- 1) Formatos estandarizados (normalizados y estructurados);
- 2) Intercambio de información por medios telemáticos; y
- 3) Conexión entre computadores.⁴¹

El intercambio de datos y documentos se realiza mediante estándares o formatos acordados o establecidos previamente por los usuarios, es decir, a través sistemas computacionales con información estructurada.

Éstos tienen un vocabulario casi universal, concebido para evitar problemas de tipo idiomático, tan comunes en la interpretación de contratos y tratados. Se trata del UN/Edifact y del ANSI ASC X 12, por ejemplo.

De esta forma, documentos como órdenes de compra, facturas, guías de despacho, etc. pueden ser entendidos de igual manera en distintos momentos y lugares.

4.2.8.3.2. Funcionamiento del EDI.

En el EDI la información se extrae directamente del sistema computacional. Luego, los documentos mercantiles, se transmiten en un formato entendible por un ordenador, utilizando la red de comunicación.⁴² En esta actividad no se utiliza papel.

Recibidos los documentos por los computadores del destinatario, los datos de tales documentos son cargados directa y automáticamente. Éstos se procesan en forma muy rápida, sin necesidad de volver a tipear la información ni de intervenirla manualmente.

4.2.8.3.3. Elementos del EDI.

Entre los elementos del EDI es posible distinguir:⁴³

a) Los *elementos subjetivos* del EDI, que son:

⁴¹ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág.78.

⁴² Cfr. Capítulo I, apartado 4.1.3. de este trabajo, donde se indicó que las redes de comunicación pueden ser públicas o privadas.

⁴³ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit, pág. 80.

1) Los usuarios.

Corresponde a los comerciantes que intercambian los mensajes electrónicos que contienen las declaraciones de voluntad, o de simple conocimiento, destinadas a la producción o ejecución de un contrato.

2) El intermediario o Centro de Compensación.

Si bien la comunicación electrónica puede realizarse en forma directa, es decir, sólo entre los computadores de los usuarios, también puede operar a través de un intermediario, quien recibe y luego transmite el mensaje al otro participante.

Se trata de una empresa o institución que provee de este servicio, y que opera mediante la gestión de un computador de su propiedad.

El Centro de Compensación debe estar siempre disponible para el usuario. Además, debe ser fiable y tener gran capacidad de comunicación. También puede ofrecer otros servicios, como auditorías, estadísticas, buzones electrónicos (para almacenar temporalmente información, lo que evita errores y problemas por la pérdida de datos), etc.

b) *Los elementos objetivos* del EDI, que son:

1) El hardware.

Consiste en un computador conectado a la red a disposición del usuario.

2) El software para EDI.

Es una aplicación informática que adapta los datos de los empresarios para ser transmitidos por la red.

3) La red de transmisión.

Ésta puede ser de voz o específica para datos.

4) Los acuerdos de intercambio.

Son celebrados entre los participantes y deben contener reglas de comunicación, jurídicas y técnicas. Pueden ser bilaterales o multilaterales, dependiendo si se celebran entre dos o varias partes.

Además, pueden contener la designación del intermediario, nombramiento que podría también acordarse en un contrato independiente para cada usuario.

4.2.8.3.4. EDI, un tipo de contratación electrónica.

El proceso mediante el cual opera el EDI es totalmente informatizado. Funciona de manera autónoma y automática en todas sus etapas: gestación, envío, aceptación e interpretación. Es un sistema propiamente electrónico.⁴⁴

El EDI reemplaza el uso del papel para los documentos comerciales más habituales. Esto se traduce en que la oferta puede no estar contenida en un documento concebido a la manera tradicional, a pesar de lo cual es perfectamente posible el acceso a ésta, ya que puede ser enviada y aceptada mediante el EDI.

El resultado de este sistema es la conclusión de contratos directamente, cualquiera que sea el lugar en que las partes se encuentren, por lo que se produce un tipo de contrato electrónico.⁴⁵

4.2.8.3.5. La normalización y la estructuración de los datos.

Ambas son las actividades que caracterizan al EDI.

1. La normalización.

Consiste en la adaptación de los lenguajes para lograr la comunicación y entendimiento entre las empresas usuarias del EDI. En otras palabras, supone una “unificación del vocabulario y de la sintaxis del mensaje a transmitir”⁴⁶, lo que se realiza a través de la creación de *normas uniformes o estándares* para el EDI.

En 1985 existían dos normas de gran aceptación. El *ASC X12* (ideado por la ANSI o *American National Standards Institute*) en Estados Unidos, y el *GTDI* (o *Guidelines for Trade Data Interchange*)⁴⁷ en Europa.

Posteriormente, y con el objeto de evitar dificultades en el comercio internacional a consecuencia de la existencia de diversos estándares incompatibles entre sí, el UN-JEDI (*United Nation's Joint EDI Comitte*) creó un lenguaje común denominado

⁴⁴ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág.132.

⁴⁵ Cfr. Capítulo I de este trabajo.

⁴⁶ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 83.

⁴⁷ Pautas para el Intercambio Comercial de Datos.

UN/EDIFACT, o simplemente, EDIFACT (*Electronic Data Interchange for Administration, Commerce and Transport*⁴⁸).

El lenguaje *EDIFACT* es un conjunto de principios y conceptos que permiten la comunicación de datos administrativos y comerciales, cualesquiera que sea el equipo informático utilizado por los participantes en el intercambio de información, y a través de todas las redes de comunicación.⁴⁹ Está conformado por un vocabulario, una gramática y directivas para la concepción de mensajes estándares, entre otras cosas.⁵⁰

Por otra parte, la Comunidad Económica Europea elaboró el *programa TEDIS* (*Trade Electronic Data Interchange Systems*) con el objeto de integrar a los distintos sectores relacionados con EDI, y así perfeccionar la infraestructura europea en materia de telecomunicaciones.

Entre los principales objetivos de este programa están:

- 1) La normalización de los mensajes EDI, mediante el desarrollo y utilización de la norma EDIFACT.
- 2) La interconexión de las redes de datos.
- 3) La elaboración de un modelo de convenio que establezca un estatuto legal de los mensajes EDI, con la finalidad de evitar los problemas jurídicos que en definitiva frenen el desarrollo de este sistema.
- 4) El establecimiento de medidas de seguridad, como la autenticación de los socios, integridad de los mensajes, confidencialidad, etc.
- 5) El estimular la industria europea de equipos y servicios de datos.

⁴⁸ Lenguaje para la Transmisión de Datos Informatizados en la Administración, el Comercio y el Transporte, de 1986.

⁴⁹ Definición de la Comisión de las Comunidades Europeas, citado por Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 83.

⁵⁰ A pesar de los esfuerzos realizados en la unificación de criterios, en la actualidad existe un gran número de *Normas* diferentes, de ámbito nacional, internacional, de diferentes sectores industriales y de organizaciones privadas: 1) las Normas ANSI (*American National Standards Institute*) que incluyen a AIAG (*Automotive Industry Action Group*), CIDX (*Chemical Industry Data Exchange*), VICS EDI (*Voluntary Interindustry Communications Standard*), y otras; 2) UN-EDIFACT de Naciones Unidas; 3) TDCC (*Transport Data Co-ordinating Committee*) para la industria ferroviaria, marítima, aérea y del automotor de Estados Unidos; 4) UCS (*Uniform Communication Standards*); GTDI (*Guidelines for Trade Data Interchange*) que incluye a Odette (*Organisation for Data Exchange by Tele Transmission in Europe*) y Tradacoms (*Trading Data Communications*), en el Reino Unido; 5) WINS (*Warehouse Information Network Standards*); etc.

2. La estructuración.

Las normas EDIFACT no sólo se refieren a la forma de los datos transferidos electrónicamente. También se ocupan del contenido de éstos, para lo que es necesario un acuerdo entre los usuarios y las administraciones.

EDIFACT board es la comisión encargada de verificar la conformidad de las transferencias electrónicas de los transportistas, la aduana y la banca con las normas internacionales.

Los mensajes EDI para transacciones comerciales adquieren la misma forma que los documentos escritos. Éstos son preparados por la EDIFACT board, y son publicados por la ONU en forma de Recomendaciones.

4.2.8.3.6. Beneficios del sistema EDI.

El uso de esta técnica se traduce en ventajas económicas importantes para las empresas que la adoptan.

Reduce considerablemente los costos derivados de la contratación, debido a que evita gastos en la etapa de negociación. Así por ejemplo, baja a cero los gastos de hoteles, pasajes y honorarios de secretarías, abogados y demás profesionales del derecho involucrados en estas actividades.

Disminuye los gastos administrativos, debido a que resulta innecesario ingresar nuevamente la información de transacciones ya almacenadas en los archivos computacionales.

Como la cantidad de empleados relacionados con el manejo de datos también se reduce, se atenúa el número de errores y retrasos propios del procesamiento manual de los documentos.⁵¹

Los beneficios también se traducen en ahorro de tiempo y papel.

Existe una cifra bastante interesante. Se estima que el 8% del costo en un envío internacional se debe al “papeleo”. Con el EDI, tal gasto baja sustancialmente.

⁵¹ Zambrano Cadena, Luis Guillermo, *La Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*, Chile, 1997, Tesis (Licenciatura en Derecho), Universidad de Concepción, Facultad de Ciencias Jurídicas y Sociales, pág. 10.

En definitiva, la adopción del EDI como mecanismo para realizar determinadas operaciones mercantiles, puede traducirse en un gran incremento de la productividad y de la competitividad de una empresa.

CAPÍTULO I.

LOS CONTRATOS ELECTRÓNICOS O DIGITALES.

1. Generalidades.

Como se comentó en la parte introductoria de este trabajo, las operaciones de comercio electrónico resultan ser muy similares a las transacciones comerciales comunes o tradicionales, con la diferencia de que algunos de sus elementos son digitales o electrónicos.

Desde un punto de vista jurídico, en cada una de estas operaciones mercantiles existirá alguna clase de contrato. Sin embargo, en las de carácter digital, tales actos se ejecutan y celebran electrónicamente, por lo que se denominan *Contratos Electrónicos*.

Esta realidad difiere, en ciertos aspectos, de la Teoría General de la Contratación, propia del documento escrito a la manera tradicional. Por ello, es posible afirmar que, en la actualidad, coexisten dos sistemas contractuales paralelos: el clásico⁵² y el electrónico (que da origen al documento electrónico).

El uso de medios digitales como la Internet genera una serie de dudas, tanto en la formulación y cumplimiento de estos contratos, así como también en la etapa precontractual o de preparación de los mismos.

Esta clase de contratación no siempre se refiere a los contratos clásicos del derecho civil, ni siquiera a aquéllos más modernos del derecho comercial. También puede tratarse de nuevas figuras, propias del comercio electrónico, las que sin sus elementos no podrían desarrollarse. Así, por ejemplo, existen los contratos de Transferencia Electrónica de Fondos (TEF), los contratos de EDI, las facturas electrónicas, los contratos marítimos y muchas otras figuras innominadas.

La contratación electrónica puede generar algunos problemas de derecho internacional, derivados de la actuación de agentes de procedencia y características

⁵² Algunos autores lo denominan sistema “*per cartam*”, Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág.120.

diferentes. Por ello, surgen ciertas dudas respecto a la legislación aplicable a estos contratos y a la jurisdicción competente para resolver sus conflictos.

La *Ley 19.799 sobre Documentos Electrónicos, Firma electrónica y Servicios de Certificación de dicha firma*⁵³ reconoce validez a los actos o contratos electrónicos. Sin embargo, les exige algunos requisitos ajenos al derecho civil clásico.

Esta norma, si bien es de gran ayuda, deja ciertas materias sin regular, como la formación del consentimiento, las que por el momento quedan entregadas a la labor jurisprudencial, mientras no encuentren solución por la vía legislativa.

La *Ley Modelo de la UNCITRAL sobre Comercio Electrónico* también se refiere a éstos, señalando 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”.⁵⁴

En los siguientes párrafos se analizará esta nueva forma de contratos. Además, se intentará aplicarles la actual normativa chilena, y se propondrán algunas soluciones a los problemas respecto de los cuales el legislador ha guardado silencio.

2. Concepto.

Conviene recordar que el contrato en general es el acto jurídico bilateral o convención que da nacimiento a obligaciones.⁵⁵ Es decir, es la manifestación de voluntad de dos o más partes realizada con la intención de crear obligaciones.

En materia contractual rige el principio de la *autonomía de la voluntad*, que permite, entre otras cosas, flexibilizar las formas contractuales, hasta el punto de autorizar la

⁵³ Ley 19.799 sobre Documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, publicada en el Diario Oficial el 12 de abril del año 2002.

⁵⁴ Ley Modelo de la UNCITRAL (Comisión de Naciones Unidas para el Derecho Mercantil Internacional) sobre Comercio Electrónico, aprobada en su vigésimo noveno período de sesiones, correspondiente al quincuagésimo primer período de sesiones de la Asamblea General de Naciones Unidas, 12 de Junio de 1996, artículo 5.

⁵⁵ Abeliuk Manasevich, René, *Las Obligaciones*, Tomo I, Tercera Edición, Editorial Jurídica de Chile, Santiago, Chile, 1993, pág. 51.

celebración de los denominados *contratos electrónicos, digitales, telemáticos*⁵⁶ o a *distancia*⁵⁷.

Estos contratos, son aquellos en que las etapas de la oferta, la aceptación y el acuerdo de voluntades se realiza mediante impulsos electrónicos (estandarizados o no), o soportados magnética o digitalmente y a distancia, entre personas ausentes, sin que exista intercambio de documentos soportados en papel.⁵⁸

3. Distinción previa.

Para evitar confusiones y delimitar el objeto del presente estudio, conviene señalar la diferencia que existe entre los *contratos electrónicos* y *la contratación informática*.

Los primeros se refieren a los contratos que, con independencia de cual sea su objeto, que puede también ser la informática, se perfeccionan a través de medios electrónicos.⁵⁹

La segunda, corresponde a los contratos de bienes y/o servicios informáticos⁶⁰, y quedan excluidos del análisis de esta memoria.

4. Elementos de los contratos electrónicos.

Tradicionalmente, en todo acto jurídico es posible encontrar determinadas condiciones de existencia y de validez.

⁵⁶ Miccoli, Mario, "Comercio telemático: una nuova realta' nel campo del diritto", 1997, <http://www.notario.it/forum/rbogot.htm>, citado por Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 134. También, Saltor, Carlos E., "Informática y Contratos", Ponencia presentada en el IV Congreso Iberoamericano de Informática y Derecho, Bariloche, 1994, citado Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., 1997, pág. 4.

⁵⁷ Directiva 97/7 CE del Parlamento Europeo y del Consejo de la UE, relativa a la protección del consumidor en materia de contratos a distancia (contrats à distance) de 17 de febrero de 1997, citada por Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág.134.

⁵⁸ Jijena Leiva, Renato Javier, "Comercio, derecho, firma y documentos digitales o electrónicos", op. cit., pág. 14.

⁵⁹ Davara Rodríguez, Miguel Ángel, *Derecho Informático*, Primera Edición, Pamplona, 1993, Ed. Aranzadi, citado por Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 4.

⁶⁰ Hernando, Isabel, "Contratos Informáticos" (Consideraciones generales), II Jornadas Abogacía e Informática, Barcelona, 21-22 abril 1994, Ilustre Colegio de Abogados de Barcelona, citado por Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 3.

Son requisitos de existencia: la voluntad, el objeto, la causa y en ciertos casos, las solemnidades. Para que un acto sea válido, se requiere, además, voluntad exenta de vicios, objeto lícito, causa lícita y capacidad de las partes.

A continuación se tratará cada uno de estos requisitos a la luz de los contratos electrónicos, con el objeto de determinar si éstos poseen o no valor jurídico desde la perspectiva del derecho civil.

4.1. La voluntad.

Tradicionalmente la voluntad se ha definido como la facultad del hombre para hacer o no hacer libremente lo que desee.⁶¹ Sin embargo, en los actos jurídicos bilaterales, y en consecuencia también en el contrato, la voluntad toma el nombre de *consentimiento*, que es el acuerdo de las voluntades de dos o más partes dirigido a lograr un resultado jurídico.⁶²

El Código Civil⁶³ no contiene normas que regulen la formación del consentimiento, por lo que esta materia se rige por los artículos 97 y siguientes del Código de Comercio⁶⁴.

4.1.1. La voluntad, base del contrato.

La utilización de medios electrónicos puede ser determinante, no sólo como vía de enlace o nexo en la celebración de un contrato, sino también como órganos decisorios frente a determinados estímulos.⁶⁵

En primer término, las partes deben acordar *el uso de medios digitales para contratar*, dejando claro el alcance que aquéllos tendrán en la contratación. En este

⁶¹ Moreno Monroy, René, *Apuntes de clases*, Derecho Civil I, Universidad de Valparaíso, 1994.

⁶² Vodanovich H., Antonio, *Curso de Derecho Civil, Parte General y los Sujetos de Derecho*, explicaciones basadas en las clases de los profesores de la Universidad de Chile, Arturo Alessandri Rodríguez y Manuel Somarriva Undurraga, Cuarta Edición, Editorial Nascimento, Santiago, Chile, 1971, pág. 325.

⁶³ Código Civil de la República de Chile, aprobado el 14 de Diciembre de 1855.

⁶⁴ Código de Comercio de la República de Chile, aprobado el 23 de Noviembre de 1865.

⁶⁵ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 7.

acuerdo previo la formación de la voluntad deberá ser libre⁶⁶, y una vez formada, no habrá inconveniente en que ésta se manifieste mediante un computador.

Incluso más, las partes podrían acordar que sus futuros contratos se realicen a través de sistemas informáticos, caso en el cual se cumplirían todas las exigencias de la legislación civil. Esto en el supuesto de que aquel sistema sirva de mero nexo para la celebración de dichos contratos.

Ahora bien, si se trata de *contratos electrónicos específicamente concluidos mediante un computador*, la voluntad de las partes, se lleva a cabo en dos instantes: en la elaboración del programa y en la etapa de comunicación o transmisión de la voluntad.⁶⁷

1. Etapa de elaboración del programa.

En esta primera fase, la voluntad tiene un carácter potencial, es decir, subyace en el programa mientras no se ejecute. Se denomina *voluntad potencial* debido a que “se encuentra latente, se ha expresado con anterioridad y se exterioriza cuando se cumplen determinados requisitos.”⁶⁸

Al elaborar el programa, las partes determinan un sistema de reglas que, de cumplirse, culminan en la celebración de un contrato.

Esta etapa puede coincidir temporalmente, y formar parte del *acuerdo previo* entre los contratantes para la celebración de sus relaciones negociales a través de medios electrónicos, pero nada impide que la creación de este programa, se haga en un momento diferente al citado acuerdo.

Según Álvarez Cienfuegos⁶⁹ este programa ya es una prueba de la existencia de las obligaciones, como expresión de la voluntad de las partes, cuando menos de manera potencial.

⁶⁶ Cfr. Capítulo I, apartado 4.1.7., de este trabajo.

⁶⁷ Guerra Balic, Jaime Tomás, trabajo de Investigación: Memoria del Doctorado 1992, “La conclusión de los contratos por medios informáticos”, citado por Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 15.

⁶⁸ Carrasco Blanc, Humberto, “Comentarios relativos a las normas sobre el consentimiento y su interacción con las nuevas tecnologías de la información”, *Revista de Derecho Informático (REDI)*, N° 98, Noviembre 2001, (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/40-16.asp> , apartado 2., letra f.

⁶⁹ Álvarez Cienfuegos, José María, “Las obligaciones concretadas por medios informáticos y la documentación electrónica de los actos jurídicos”, ponencia para el III Congreso Iberoamericano de Informática y Derecho, Mérida, 1992, Actas, Volumen II. *Revista Informática y Derecho*, 5, UNED, Centro Regional de Extremadura, Mérida, 1994. Aranzadi Editorial; citado por Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 15.

2. Comunicación de la voluntad.

La segunda etapa supone la ejecución del citado programa, como *voluntad expresada*. En ella se estará declarando la voluntad, y con esto perfeccionando el contrato.

Al acontecer una serie de situaciones de hecho (precio, número de unidades en venta, etc.), el ordenador automáticamente ejecuta el contrato celebrado. En estos casos “las partes asumen una obligación condicional que dependerá de un acontecimiento futuro e incierto, pero no se volverá a manifestar la voluntad en un momento posterior. La voluntad de los contratantes se manifestó en el primer momento.”⁷⁰

A pesar de lo señalado, en la mayor parte del comercio electrónico, y especialmente en el denominado “empresa-consumidor”, estas etapas dejan paso a contratos de adhesión.

4.1.2. La adhesión.

Los *contratos de adhesión* juegan un importante rol en el comercio electrónico.

Éstos son aquéllos en los que las condiciones de reglamentación son obra de una sola de las partes (del oferente), de manera que el contrayente no colabora de manera alguna en la formación del contenido contractual. En otras palabras, no existe una verdadera negociación, sino un simple acto de aceptación o adhesión de las condiciones predeterminadas en forma unilateral.⁷¹

Los contratos de adhesión son muy utilizados en las transacciones comerciales incluidas las de comercio electrónico. Su utilidad radica, principalmente, en la eliminación del tiempo necesario para efectuar negociaciones individuales, lo que se traduce también en ahorro de costos.

El oferente es el mayor beneficiado en este tipo de contratación, debido a que determina los términos del contrato. Por ello, el legislador debe, necesariamente,

⁷⁰ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 12.

⁷¹ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 8.

intervenir para proteger los intereses de la contraparte, a fin de evitar la inclusión de cláusulas abusivas.

La *Ley Modelo de la UNCITRAL sobre Comercio Electrónico* no hace referencia a esta clase de contratos, con el objeto de evitar contradicciones con la normativa sobre protección a los consumidores de los distintos países.

En Chile, esta materia está regulada por el párrafo 4° de la *Ley 19.496* (o *Ley del Consumidor*)⁷², donde se establecen algunas normas de equidad para las estipulaciones y el cumplimiento de los contratos de adhesión.

A pesar de que la ley no hace una alusión específica a los contratos de adhesión celebrados a través de medios digitales, los conceptos legales, además de las normas relacionadas con éstos, les serían perfectamente aplicables.^{73 74}

Sin embargo, a pesar de la amplitud de tales conceptos, éstos quedarían limitados por el artículo 2° inciso primero, que indica que “sólo quedan sujetos a las disposiciones de esta ley los actos jurídicos que, de conformidad a lo preceptuado en el Código de Comercio u otras disposiciones legales, tengan el carácter de mercantiles para el proveedor y civiles para el consumidor”.

Esta disposición vendría a restringir la aplicación de esta ley sólo “a aquellos actos que revistan el carácter de mercantiles para el proveedor y civiles para el consumidor, por lo que quedarían fuera de su ámbito aquellas situaciones en que el usuario celebra un acto que en si es civil, pero que por tener el usuario una actividad principal mercantil transforma ese acto en comercial en virtud del principio de accesoriedad”.⁷⁵

No obstante lo señalado, existe cierta jurisprudencia que no aplicaría el principio de la accesoriedad indicado, aplicando la citada Ley del Consumidor a aquellas situaciones

⁷² Ley 19.496 que establece normas sobre protección de los derechos de los consumidores, publicada en el Diario Oficial el 7 de marzo de 1997.

⁷³ El artículo 1 inciso 2°, N° 6 de la Ley 19.496 define contrato de adhesión como “aquel cuyas cláusulas han sido propuestas unilateralmente por el proveedor sin que el consumidor, para celebrarlo, pueda alterar su contenido.”

⁷⁴ El artículo 1 inciso 2°, N° 1 y N° 2 de la Ley 19.496 establecen que “Para los efectos de esta ley se entenderá por: 1) Consumidores: Las personas naturales o jurídicas que, en virtud de cualquier acto jurídico oneroso, adquieran, utilicen o disfruten, como destinatarios finales, bienes o servicios. 2) Proveedores: las personas naturales o jurídicas, de carácter público o privado, que habitualmente desarrollen actividades de producción, fabricación, importación, construcción, distribución o comercialización de bienes o de prestación de servicios a consumidores, por las que se cobre precio o tarifa”.

⁷⁵ Carrasco Blanc, Humberto, “Contratos informáticos y Ley del Consumidor Chilena”, *Revista de Derecho Informático (REDI)*, N° 15, Octubre 1999, (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/revista.asp?idRevista=17> , apartado A 1).

en que el acto es civil para el consumidor comerciante (pudiendo ser mercantil en virtud del principio expresado) y mercantil para el proveedor.⁷⁶

4.1.3. Oferta y Aceptación.

Al igual que en la contratación clásica, el consentimiento en los contratos electrónicos se produce por el concurso de la oferta y la aceptación. Sin embargo, en este caso, ambas se realizan por medios electrónicos.

4.1.3.1. La oferta o policitud electrónica.

Es la proposición que una o más personas realizan a través de medios digitales de comunicación para celebrar una determinada convención.

Sobre la base de las normas del Código de Comercio chileno, es posible distinguir diversas *clases de oferta electrónica*:

a) Verbal o escrita.

La policitud electrónica generalmente es escrita.

Sin embargo, también pueden existir algunas de carácter verbal, como por ejemplo, las que se realizan a través de videoconferencias.⁷⁷

b) Expresa o tácita.

La propuesta electrónica puede ser efectuada de ambas maneras.

⁷⁶ Se trata de una sentencia de la Corte de Apelaciones de Concepción, del 2 de Marzo de 1999, donde se aplicó la Ley del Consumidor a la causa caratulada Gonzalez con Sociedad Comercial Kaufmann S.A., Rol N° 85-98, en la que el demandante había adquirido un camión a la demandada, que se dedicaba a la compraventa de vehículos motorizados, teniendo el demandante como actividad principal el transporte de madera. En todo caso, el tribunal no se refirió expresamente sobre esta cuestión condenando a la demandada en virtud de la citada Ley. Carrasco Blanc, Humberto, “Contratos informáticos y Ley del Consumidor Chilena”, op. cit., nota 5.

⁷⁷ Carrasco Blanc, Humberto, “Comentarios relativos a las normas sobre el consentimiento y su interacción con las nuevas tecnologías de la información”, op. cit., apartado 2., letra h.

c) A persona determinada o indeterminada.

El comercio electrónico, en la mayoría de los casos, se realiza a través de ofertas al público en general (o indeterminadas). En virtud de lo establecido en el artículo 105 del Código de Comercio, la doctrina atribuye escaso valor a este tipo de propuestas.⁷⁸

Sin embargo, en la actualidad, las ofertas (incluidas las electrónicas) a personas determinadas e indeterminadas también se encuentran reguladas por la *Ley 19.496*⁷⁹, siempre que se reúnan los requisitos para su aplicación. Esta disposición, otorga “una nueva regulación a las ofertas al público, con lo que podríamos sostener que se estaría modificando el criterio en cuanto al valor de las ofertas a personas indeterminadas dejando de tener una obligatoriedad relativa”.⁸⁰

Ahora bien, si se considera el *medio* utilizado por el proponente, las ofertas electrónicas pueden clasificarse en:

a) Las realizadas a través de e-mail.

Estas propuestas son enviadas al correo electrónico de determinadas personas.

Sin embargo, en la mayor parte de los casos, corresponde a una *mailing list*, es decir, a listas de correos a los que se les envía información, las que no debieran ser consideradas ofertas a personas determinadas.⁸¹

b) Las efectuadas en línea o en redes de comunicaciones, como Internet.

Se trata de las ofertas que se encuentran en forma permanente en las redes.

Éstas no llegan a un ordenador determinado sino que se accede a ellas mediante el ingreso a diversas páginas Web, por lo que constituyen ofertas a personas indeterminadas.

⁷⁸ Código de Comercio, artículo 105: “Las ofertas indeterminadas contenidas en circulares, catálogos, notas de precios corrientes, prospectos, o en cualquier otra especie de anuncios impresos, no son obligatorias para el que las hace”.

⁷⁹ Ley 19.496 que establece Normas sobre Protección de los Derechos de los Consumidores, publicada en el Diario Oficial el 7 de marzo de 1997.

⁸⁰ Carrasco Blanc, Humberto, “Comentarios relativos a las normas sobre el consentimiento y su interacción con las nuevas tecnologías de la información”, op. cit., apartado 2., letra h, (Aplicación de las normas nacionales a la formación del consentimiento electrónico), 1).

⁸¹ Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, op. cit., pág. 17.

4.1.3.2. La aceptación electrónica.

Es la declaración de voluntad que una persona efectúa mediante algún medio digital de comunicación, manifestando su conformidad con la proposición que se le formula.

De la misma manera que la oferta, la aceptación *puede clasificarse en*:

a) Expresa o tácita.

La tácita produce los mismos efectos que la expresa, según el artículo 103 del Código de Comercio.⁸²

b) Pura y simple, y condicional.

La aceptación pura y simple es la que demuestra total concordancia con la oferta realizada.

La condicional, es la que se emite con reservas, modificando los términos de la oferta.⁸³ Ésta constituye una nueva oferta.⁸⁴

Existen, además, ciertos *requisitos de la aceptación* necesarios para la formación del consentimiento.

1) Debe darse mientras la oferta se encuentre vigente.

La oferta deja de estar vigente por dos causas:

a) Retractación del proponente.

El oferente tiene la posibilidad de revocar o dejar sin efecto la propuesta mientras no haya aceptación.

En la oferta en línea, por su carácter permanente, es difícil que haya retractación. Generalmente el cliente adquiere un bien o servicio en el mismo momento en que accede a la página que contiene la propuesta.

Sin embargo, la retractación del oferente puede producirse en el caso que el individuo no celebre el contrato en el momento de conocer dicha oferta. Por ejemplo, decide pensar sobre la conveniencia o no de aceptar, y planea acceder a la página

⁸² El artículo 103 del Código de Comercio establece: “La aceptación tácita produce los mismos efectos y está sujeta a las mismas reglas que la expresa”.

⁸³ Carrasco Blanc, Humberto, “Comentarios relativos a las normas sobre el consentimiento y su interacción con las nuevas tecnologías de la información”, op. cit., apartado 2., letra h, (Aplicación de las normas nacionales a la formación del consentimiento electrónico), 2).

⁸⁴ El artículo 102 del Código de Comercio señala: “La aceptación condicional será considerada como una propuesta”.

nuevamente con posterioridad. En esta situación, el sitio podría haber modificado la oferta, o simplemente no estar.⁸⁵

Respecto a la oferta vía e-mail, resulta perfectamente aplicable el artículo 99 del Código de Comercio, según el cual, el proponente puede retractarse, siempre que no se haya “comprometido a esperar contestación o a no disponer del objeto del contrato, sino después de desechada o de transcurrido un determinado plazo”.⁸⁶

El mismo Código dispone que si se produce retractación tempestiva de la oferta, el proponente deberá pagar al aceptante los gastos y perjuicios que hubiere sufrido. Sin embargo, podrá eximirse del pago de la obligación de indemnizar si cumple el contrato ofrecido.⁸⁷

b) Muerte o incapacidad legal del proponente.

En la contratación electrónica generalmente intervienen personas jurídicas, por lo que estas causales tienen poca aplicación.

2) Debe ser oportuna.

La aceptación debe otorgarse dentro del *plazo legal o voluntario* señalado por el proponente.

a) Plazo voluntario.

En esta situación se estará al término establecido por el oferente.

b) Plazo legal.

Para su determinación, se diferencia entre propuestas verbales y escritas.

b.1.) En las ofertas verbales, la aceptación debe darse en el acto de ser conocida.⁸⁸

b.2.) En las escritas, se distingue, a su vez:⁸⁹

⁸⁵ Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, op. cit., pág. 18.

⁸⁶ Código de Comercio, artículo 99.

⁸⁷ Código de Comercio, artículo 100.

⁸⁸ El artículo 97 del Código de Comercio señala: “Para que la propuesta verbal de un negocio imponga al proponente la respectiva obligación, se requiere que sea aceptada en el acto de ser conocida por la persona a quien se dirigiere; y no mediando tal aceptación, queda el proponente libre de todo compromiso”.

⁸⁹ El artículo 98 del Código de Comercio establece: “La propuesta hecha por escrito deberá ser aceptada o desechada dentro de veinticuatro horas, si la persona a quien se ha dirigido residiere en el mismo lugar que el proponente, o a vuelta de correo, si estuviere en otro diverso”.

b.2.1.) Si la persona ofertada se encuentra en el mismo lugar del proponente, la oferta debe ser aceptada o rechazada en un plazo de veinticuatro horas.

Esta solución es perfectamente aplicable a la contratación electrónica, pero sólo en lo relativo a aquellas ofertas enviadas a través de e-mail.⁹⁰ Las ofertas en línea, no son enviadas al ofertado, sino que “éste llega a ellas”, por lo que es discutible la aplicación de esta norma en esta clase de propuestas.

Este término de veinticuatro horas ¿se cuenta desde que el aceptante recibe la oferta en su buzón electrónico asignado por el servidor o desde que el mensaje ingresa a su computador?

En este caso es necesario que dicho mensaje sea recibido por el ordenador. Sin embargo, ello debería ser determinado por el legislador en una norma específica.

b.2.2.) Si los involucrados se encuentran en lugares distintos, la oferta deberá ser aceptada a “vuelta de correo”.

Esta parte de la disposición no es aplicable a la contratación electrónica, debido a que en ésta no existe mayor diferencia en la velocidad de respuesta de los mensajes de personas que se encuentran en la misma ciudad o en ciudades distintas.

En definitiva, la distinción anteriormente señalada, no es necesaria en la contratación electrónica.

3) Debe ser pura y simple.

La aceptación deberá acoger la oferta en todas sus partes, sin modificación alguna. De no ser así, no se forma el consentimiento.⁹¹

Si la aceptación es condicional, será considerada como una nueva propuesta.⁹²

A modo de conclusión conviene señalar que es necesario efectuar una modificación al Código de Comercio, con el objeto de adecuar sus normas a las nuevas situaciones de la sociedad de la información.

⁹⁰ Carrasco Blanc, Humberto, “Comentarios relativos a las normas sobre el consentimiento y su interacción con las nuevas tecnologías de la información”, op. cit., apartado 2., letra h (Aplicación de las normas nacionales a la formación del consentimiento electrónico).

⁹¹ El artículo 101 del Código de Comercio dispone: “Dada la contestación, si en ella se aprobare pura y simplemente la propuesta, el contrato queda en el acto perfeccionado y produce todos sus efectos legales (...)”.

⁹² Código de Comercio, artículo 102.

Otra posibilidad, es dictar una normativa especial que dé pautas claras sobre estas materias. La *Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma*, en el artículo 3, reconoce validez a los contratos suscritos por medio de firma electrónica, pero nada dice respecto a la oferta y a la aceptación.

La *Ley Modelo de la UNCITRAL sobre Comercio Electrónico*, en su artículo 11, reconoce de manera expresa la posibilidad que la oferta y la aceptación sean expresadas por medio de un mensaje de datos. Sin embargo, no entra en detalles, por lo que requiere ser completada en algunos aspectos.

4.1.4. Momento de formación del consentimiento.

Este punto es de gran trascendencia debido a que los contratos, salvo excepciones, “se entienden pactados en el momento en que se forma el consentimiento”.⁹³

A partir de este instante, se derivan una serie de efectos jurídicos importantes, como por ejemplo:

- 1) Se pueden apreciar las condiciones de validez de la voluntad, especialmente la capacidad de las partes para contratar;
- 2) Determina si hay o no objeto ilícito;
- 3) Los derechos y obligaciones que nacen de un contrato pueden ser ejercidos o demandados por la contraparte;
- 4) Determina la legislación aplicable, esto es, la que estuviere vigente al momento de celebración del contrato;
- 5) Se termina el derecho a revocar la oferta;
- 6) Fija el instante a partir del cual comienza a correr el tiempo para la prescripción o la caducidad de ciertas acciones.

Para establecer el momento en que se forma el consentimiento en los contratos electrónicos, se deberá determinar si éstos son *contratos celebrados entre presentes o contratos celebrados entre ausentes*.

⁹³ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op. cit., pág.30.

Conviene recordar que existen dos *criterios para diferenciar a ambas clases de contratos*. Uno atiende a si ambas partes se encuentran en el mismo lugar, y el otro a si la aceptación puede ser conocida por la contraparte inmediatamente después de ser emitida.

Según el primer punto de vista, los contratos entre presentes son aquellos que se celebran entre partes que se encuentran en un mismo lugar. Por el contrario, en los contratos entre ausentes, las partes se encuentran en lugares distintos.⁹⁴

En virtud del segundo criterio, los contratos entre presentes “son aquellos en que la aceptación puede ser conocida por la otra parte al tiempo o inmediatamente de ser emitida”, mientras que los contratos entre ausentes son “aquellos en que la aceptación puede ser conocida por el oferente sólo después de cierto tiempo, más o menos largo, de ser formulada”.⁹⁵

Siguiendo este segundo criterio, los contratos electrónicos *generalmente se consideran contratos celebrados entre ausentes, sin perjuicio de existir casos en que se les consideran celebrados entre presentes*⁹⁶(por ejemplo, los celebrados a través de videoconferencias o de telefonía de voz sobre IP).⁹⁷

Ahora bien, si se equipara la comunicación a través del Internet *al contacto telefónico*, en el sentido de que en ambos casos, a pesar de que las partes se encuentran físicamente separadas, es posible un conocimiento instantáneo de la aceptación, se trataría de un contrato *entre presentes*, por lo que no habría dificultad en determinar el momento en que el consentimiento se entiende formado.

Sin embargo, los contratos celebrados mediante la Internet también podrían ser catalogados como celebrados *entre ausentes*, si existe un lapso entre la oferta y la aceptación. En este caso, habría que determinar en qué momento se forma el consentimiento.

⁹⁴ Vodanovich H., Antonio, *Curso de Derecho Civil, Parte General y los Sujetos de Derecho*, op. cit., pág. 350.

⁹⁵ Vodanovich H., Antonio, *Curso de Derecho Civil, Parte General y los Sujetos de Derecho*, op. cit., pág. 350.

⁹⁶ Magliona Markovitch, Claudio Paul, “Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico”, *Revista de Derecho Informático (REDI)*, N° 34, Mayo 2001 (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/35-9.asp> , apartado 2., letra b).

⁹⁷ De esta manera, “la regla general en la contratación electrónica es que sean contratos entre ausentes, con algunas excepciones en que son entre presentes”. Carrasco Blanc, Humberto, “Comentarios relativos a las normas sobre el consentimiento y su interacción con las nuevas tecnologías de la información”, op. cit., apartado 2., letra d (Contratación electrónica ¿contrato entre presentes o ausentes?).

Muchas de las operaciones comerciales electrónicas se realizan de esta forma. Esto ocurre en las que utilizan instrumentos como el correo electrónico, situación que podría equipararse “a los contratos celebrados por correo u otros medios de comunicación a distancia no instantáneos”.⁹⁸

Tradicionalmente la doctrina reconoce cuatro soluciones que pretenden determinar el momento de formación del consentimiento en los contratos celebrados entre ausentes. Éstas se refieren, en orden cronológico, a los siguientes instantes:

1. Perfección del contrato en el momento en que el destinatario de la oferta da su aceptación, aunque ésta no sea conocida por el oferente.
2. Perfección del contrato en el momento en que el ofertado envía el documento o mensaje que contiene la aceptación.
3. Perfección del contrato en el momento en que el oferente recibe el documento que contiene la aceptación, y
4. Perfección del contrato en el momento en que el oferente toma conocimiento de la aceptación.

Se trata, respectivamente, de las teorías de la aceptación o declaración, de la expedición o remisión, de la recepción y de la información o del conocimiento.

El ordenamiento jurídico chileno, salvo ciertas excepciones, se adhiere a la *teoría de la aceptación*⁹⁹, es decir, el consentimiento se entiende formado cuando el destinatario de la oferta la acepta, sin que sea necesario que el proponente se entere de la aceptación.

La *Ley 19.799 sobre Documentos electrónicos, Firma electrónica y Servicios de Certificación de dicha firma*, no se refiere a este tema, por lo que es aplicable, respecto a los contratos electrónicos, esta solución general dada por el Código de Comercio para las otras formas de contratos.

De esta manera, “el mero hecho de que la persona acepte, sin entrar siquiera a analizar si efectivamente contesta la oferta, o cómo, o cuándo lo hace, sería el elemento que determine la formación del consentimiento”¹⁰⁰ en los contratos digitales.

Sin embargo, al parecer, la adopción de la teoría de la aceptación en los contratos electrónicos no es la mejor solución, debido a que surge el problema de determinar qué se entiende por aceptación.

⁹⁸ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op. cit., pág. 31.

⁹⁹ Cfr. Código de Comercio, artículo 101.

¹⁰⁰ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op. cit., pág. 31.

Sería más adecuado adoptar un *sistema que exija una manifestación externa de dicha aceptación* para evitar posibles conflictos y conclusiones equivocadas. Así, lo mínimo que debiera requerirse es que sea enviada al oferente.¹⁰¹

De esta forma, por ejemplo, se ha señalado que en el contrato modelo de EDI para la Comunidad Europea “una operación se considerará perfeccionada en el momento (...) en que un mensaje estandarizado generado por el emisor se haya hecho disponible (haya sido recepcionado) al sistema de información del receptor, sin necesidad de que posteriormente haya un acuse recibo o una manifestación de aceptación”.¹⁰²

La *Ley Modelo sobre Comercio Electrónico de UNCITRAL* tampoco indica el momento en que debe entenderse perfeccionado el consentimiento, con el objeto de evitar las contradicciones con el derecho interno de los distintos estados a propósito de esta materia. Sin embargo, entrega ciertas normas para la determinación del tiempo del envío y la recepción de los mensajes de datos.

Así, el artículo 15 establece el momento en que *se entiende enviado 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*”.

Esta solución parece bastante lógica, especialmente si se basa en la utilización del correo electrónico. Sin embargo, no parece tener mucha aplicación en los ordenamientos que suscriben la teoría de la aceptación, como el derecho chileno.

En el número dos del artículo 15 se define el *momento de la recepción*. En este caso hay que distinguir si ha habido o no un acuerdo entre el iniciador y el destinatario respecto al momento de la recepción.

Si ha habido un convenio, debe estarse a éste. Por el contrario, si las partes nada han pactado, se subdistingue:

a) Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción se producirá en el momento en que el *mensaje entre en el sistema de información* designado.

¹⁰¹ Ibid.

¹⁰² Jijena Leiva, Renato Javier, “Comercio electrónico y derecho. La problemática jurídica del Comercio Electrónico”, op.cit. apartado III, 3.1.

Pero si éste es enviado a un sistema de información distinto al designado, la recepción tendrá lugar en el momento en que el destinatario recupere el mensaje de datos, es decir, cuando lo recibe.

b) Si el destinatario no ha designado un sistema de información, la recepción se producirá al entrar el mensaje de datos en cualquiera de los sistemas de información del destinatario.

En conclusión, si bien la Ley Modelo de la UNCITRAL no se pronuncia por ninguna de las cuatro teorías señaladas anteriormente, del contenido del artículo 15 se deduce que prefiere aplicar la teoría del envío del mensaje, o de la recepción del mensaje, “aprovechando la facilidad de comunicación a través de Internet para otorgar una mayor seguridad a estas transacciones electrónicas.”¹⁰³

4.1.5. Lugar de formación del consentimiento.

La importancia de determinar el lugar donde se entiende formado el consentimiento, y en consecuencia, donde se tendrá por celebrado el contrato, radica en que:

- 1) Fija la competencia de los tribunales;
- 2) Determina la legislación aplicable;
- 3) Señala los usos o la costumbre que tiene cabida en los casos en que la voluntad puede ser interpretada de acuerdo a ellos.¹⁰⁴

Este tema constituye otra de las controversias del comercio electrónico.

Tradicionalmente la legislación chilena ha admitido que “el lugar en donde se entiende formado el consentimiento está determinado por la *ubicación del aceptante*”.^{105 106}

Sin embargo, al igual como se comentó en el tema anterior, la solución dada por el Código de Comercio aplicada a los contratos electrónicos, resulta poco adecuada.

¹⁰³ Otero Alvarado, Jorge y Lanckenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit., pág. 33.

¹⁰⁴ Vodanovich H., Antonio, *Curso de Derecho Civil, Parte General y los Sujetos de Derecho*, op. cit., pág. 355.

¹⁰⁵ Magliona Markovicth, Claudio Paul, “Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico”, op. cit., apartado 2., letra b).

¹⁰⁶ El artículo 104 del Código de Comercio señala: “Residiendo los interesados en distintos lugares, se entenderá celebrado el contrato, para todos sus efectos legales, en el de la residencia del que hubiere aceptado la propuesta primitiva o la propuesta modificada”.

Lo anterior se debe a que el comercio electrónico, por sus especiales características, puede ocasionar ciertas dificultades en la determinación del lugar donde ocurre la transacción.

En ciertas ocasiones, el sitio donde está el sistema que envía o recibe el mensaje de datos es diferente de aquél donde se encuentra la persona que lo envió o recibió. En otras palabras, puede haber un problema técnico para definir cuál es ese lugar.¹⁰⁷

La *Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma*, no se refiere al lugar en que se forma el consentimiento de los contratos electrónicos, por lo que se hace necesaria una modificación legal en este aspecto.

Con el objetivo de respetar las soluciones dadas por los estados respecto a este tema, la *Ley Modelo de UNCITRAL sobre Comercio Electrónico* no dice dónde se entiende formado el consentimiento en los contratos electrónicos.¹⁰⁸ Habla del *lugar donde se considera enviado y recibido el mensaje de datos*.

Así, el artículo 14 señala que “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.”

Esta norma, plantea el inconveniente de que no define específicamente qué se entiende por “lugar de establecimiento”. Sin embargo, a pesar de ello, la solución es bastante acertada, en el sentido que mantiene la tradicional designación utilizada por los ordenamientos jurídicos respecto al lugar donde ocurren las transacciones comerciales.

Con el objeto de evitar conflictos en relación al tema tratado, se debe aplicar el sistema que considera formado el consentimiento una vez que el oferente recibe y tiene

¹⁰⁷ Por otro lado, hay autores que opinan que “el ciberespacio es en sí un todo”. Esto quiere decir que los mensajes no cambiarían de lugar geográfico, debido a que nunca dejan el ciberespacio (Cfr. Introducción, apartado 4.1.4.). Sin embargo, esta teoría sólo podría tener aplicación en aquellos casos en que los mensajes no ingresan al sistema de información del receptor, a través de lo que se conoce como “download”, ya que en esta situación, estarían saliendo del ciberespacio. Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit., pág. 34.

¹⁰⁸ Lo mismo ocurre respecto al momento de formación del consentimiento (Cfr. Capítulo I, 4.1.4.).

a su disposición el mensaje que contiene la aceptación. Aplicando la Ley Modelo, este lugar sería donde el receptor tenga el asiento principal de sus negocios.

Utilizando esta misma solución se evitan también los problemas y dudas respecto al momento en que se forma este consentimiento.

4.1.6. El consentimiento en los contratos reales y solemnes.

Hasta ahora todo lo dicho a propósito de la voluntad es aplicable a los contratos consensuales, es decir, a aquellos que se perfeccionan por el solo consentimiento.¹⁰⁹ Sin embargo, conviene hacer ciertas observaciones respecto a las otras clases de contratos reconocidas por el derecho chileno: los reales y los solemnes.

Es importante recordar que los *contratos reales* son aquellos que para ser perfectos requieren además del consentimiento, la tradición de la cosa a que se refiere.¹¹⁰

El consentimiento se perfecciona de la misma manera que en los contratos consensuales, por lo que las normas relativas a la oferta y aceptación, les son plenamente aplicables. Sin embargo, por exigencia del legislador, es necesaria la entrega de la cosa para entender perfecto el contrato.

Por esto último, Humberto Carrasco¹¹¹ descarta la posibilidad de perfeccionar contratos reales por la vía electrónica, ya que no sería posible hacer la entrega.

Sin embargo, si la cosa es de carácter intangible, sería perfectamente posible efectuar la entrega electrónicamente. Así, por ejemplo, en el caso de un mutuo de dinero realizado mediante una Transferencia Electrónica de Fondos la entrega puede hacerse a través de una acreditación de dinero en la cuenta del mutuario, por lo que el contrato quedaría perfecto en línea.

Por otro lado, existen los *contratos solemnes*, los que además del consentimiento, necesitan del cumplimiento de ciertas formalidades especiales, de manera que sin ellas no producen ningún efecto civil.

¹⁰⁹ Código Civil, artículo 1443.

¹¹⁰ El Artículo 1443 del Código Civil dice que “el contrato es real cuando, para que sea perfecto, es necesaria la tradición de la cosa a que se refiere.” El profesor Abeliuk, señala que el Código comete una impropiedad al hablar de tradición, debido a que ésta es un modo de adquirir el dominio, y en los contratos reales la regla general es que, quien recibe la cosa, es un mero tenedor, con excepción del mutuo en que sí hay tradición. Por ello observa que sería más adecuado definirlos como aquellos perfeccionados por la entrega de la cosa. Abeliuk Manasevich, René, *Las Obligaciones*, Tomo I, op. cit., pág.73.

¹¹¹ Carrasco Blanc, Humberto, “Comentarios relativos a las normas sobre el consentimiento y su interacción con las nuevas tecnologías de la información”, op. cit., apartado 2., letra e.

Se debe cumplir con una solemnidad objetiva, es decir, requerida en relación al acto en sí mismo, e igual para todos los contratos de idéntica naturaleza. Puede tratarse del otorgamiento de una escritura pública (como en la compraventa de bienes raíces o en la hipoteca), instrumentos privados (caso de la promesa), concurrencia de algún ministro de fe, o testigos (como en el matrimonio), etc.¹¹²

La inobservancia de este tipo de solemnidad, produce nulidad absoluta del contrato en virtud del artículo 1682 del Código Civil.¹¹³ Más aún, en doctrina provoca inexistencia del mismo.

En consecuencia, y de acuerdo a lo expresado, es necesario dar cumplimiento a las solemnidades dispuestas por el legislador para que se perfeccionen los contratos solemnes. En este punto adquiere gran relevancia el desarrollo del documento electrónico y de sus sistemas de seguridad, para que pueda dar plena fe de los actos y contratos que contenga. Para ello, resulta primordial considerar la posibilidad de una modificación legal en torno a la implementación de notaría electrónica para su otorgamiento, las que los dotarían de pleno valor.¹¹⁴

La ley 19.799 sobre Documentos electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma, en su artículo 3, reconoce validez a los actos y contratos suscritos por medio de firma electrónica. Sin embargo, en el inciso 2º, descarta aquellos a los que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, a los que la ley requiere la concurrencia personal de alguna de las partes y los relativos al derecho de familia. En el artículo 4 agrega que, los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada.

De lo anterior se puede deducir que, en la actualidad, a diferencia de lo que opina Humberto Carrasco¹¹⁵, es posible celebrar algunos contratos solemnes de manera electrónica, esto es, aquellos susceptibles de cumplirse mediante firma electrónica simple o calificada. Sin embargo, la ley es poco clara al respecto. Es necesaria una reforma legislativa en el ámbito notarial y registral que implemente instituciones como el Notario y el Conservador electrónico.

¹¹²Abeliuk Manasevich, René, *Las Obligaciones*, Tomo I, op. cit., pág. 71.

¹¹³ El artículo 1982 del Código Civil establece que: "...la nulidad producida por la omisión de algún requisito o formalidad que las leyes prescriben para el valor de ciertos actos o contratos en consideración a la naturaleza de ellos, (...), son nulidades absolutas."

¹¹⁴ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág.151.

¹¹⁵ Carrasco Blanc, Humberto, "Comentarios relativos a las normas sobre el consentimiento y su interacción con las nuevas tecnologías de la información", op. cit., apartado 2., letra e.

4.1.7. Vicios del consentimiento.

Para la validez de los contratos, se requiere entre otros requisitos, que el consentimiento esté exento de vicios. *Vicio* será todo lo que impida la libertad y conciencia en su formación.

Los vicios de que puede adolecer el consentimiento son: el error, la fuerza y el dolo.¹¹⁶

Éstos pueden adquirir ciertos matices en los contratos electrónicos.

4.1.7.1. Error.

El Código Civil¹¹⁷ no define el error, por lo que recurriendo a la doctrina, se puede señalar que es la ignorancia o falso concepto que se tiene de la realidad.¹¹⁸

En los contratos electrónicos, la voluntad se dirige a aspectos y elementos que en la contratación clásica no plantearía inconveniente alguno.

Además, el diálogo entre las partes es mucho menor, e incluso en ocasiones, estandarizado, por lo que el error puede aparecer con más frecuencia.¹¹⁹

El error como vicio de la voluntad puede presentarse tanto en el acuerdo previo en que las partes optan que su contratación sea digital, como en la formación del programa (si se da en un momento diferente a dicho acuerdo) y en la ejecución del mismo.¹²⁰

En el Código Civil chileno se distingue entre error de hecho y error de derecho.

El *error de derecho*, que es la ignorancia o concepto equivocado que se tiene de una norma jurídica,¹²¹ no vicia el consentimiento según el artículo 1452.

¹¹⁶ Así lo dice el artículo 1451 del Código Civil.

¹¹⁷ El Código Civil regula el error entre los artículos 1453 al 1455 inclusive.

¹¹⁸ Moreno Monroy, René, op. cit.

¹¹⁹ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 16.

¹²⁰ Cfr. con la distinción realizada en “La voluntad, base del contrato.” Capítulo I, apartado 4.1.1 de este estudio.

¹²¹ Vodanovich H., Antonio, *Curso de Derecho Civil, Parte General y los Sujetos de Derecho*, op. cit., pág. 358.

Sin embargo, hay legislaciones en las que el criterio es diferente. En la libanesa, por ejemplo, el error de derecho vicia el consentimiento.¹²² En cambio en España, ha sido la jurisprudencia la que en forma muy estricta lo ha reconocido como causa de anulación del contrato.¹²³

El *error de hecho*, es decir, la ignorancia o concepto equivocado que se tiene de una cosa o de un hecho, vicia el consentimiento en los casos señalados por los artículos 1453, 1454 y 1455 del Código Civil.¹²⁴

En los contratos electrónicos las características del error, si bien sustancialmente son las mismas que en la contratación tradicional, están revestidas de matices bastante peculiares.¹²⁵

Un error en el programa puede producir divergencia entre lo contratado y lo deseado. En otras palabras, la automatización puede hacer más complicada la determinación de las características del objeto del contrato, lo que puede impedir que se detecten circunstancias que harían que una de las partes no llegase a ejecutarlo, y con ello, a la perfección del negocio. El error puede producirse, también, en el diálogo entre los operadores electrónicos, provocando las mismas consecuencias.¹²⁶

Respecto al error en la persona, éste puede producirse con mayor facilidad. Esto debido a que las partes no tienen contacto directo. Sin embargo, gracias a los códigos o claves de acceso este problema ha disminuido notoriamente.¹²⁷

4.1.7.2. Fuerza.

Según el Código la fuerza vicia la voluntad, “cuando es capaz de producir una impresión fuerte en una persona de sano juicio, tomando en cuenta su edad, sexo y

¹²² Vodanovich H., Antonio, *Curso de Derecho Civil, Parte General y los Sujetos de Derecho*, op. cit., pág. 359.

¹²³ Sentencia, 6 de abril de 1962 y 7 de julio de 1981, Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 17.

¹²⁴ Artículo 1453: “(...) cuando recae sobre la especie de acto o contrato que se ejecuta o celebra (...) o sobre la identidad de la cosa específica de que se trata (...)”. Artículo 1454: “(...) cuando la sustancia o calidad esencial del objeto sobre que versa el acto o contrato, es diversa de lo que se cree (...). El error acerca de cualquier otra calidad de la cosa no vicia el consentimiento (...), sino cuando esa calidad es el principal motivo de una de ellas para contratar, y este motivo ha sido conocido de la otra parte”. Artículo 1455: “El error acerca de la persona con quien se tiene intención de contratar no vicia el consentimiento, salvo que la consideración de esta persona sea la causa principal del contrato”.

¹²⁵ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 19.

¹²⁶ Ibid.

¹²⁷ Cfr. con lo señalado a propósito de la capacidad, Capítulo I, apartado 4.2. de este trabajo.

condición.” Además, señala que “se mira como una fuerza de este género todo acto que infunde a una persona un justo temor de verse expuesta a ella, su consorte o alguno de sus ascendientes o descendientes a un mal irreparable y grave”.¹²⁸ Ahora bien, “el *temor reverencial*, esto es, el solo temor de desagradar a las personas a quienes se debe sumisión y respeto, no basta para viciar el consentimiento.”¹²⁹

El artículo 1457 agrega que, para que la fuerza vicie el consentimiento, no se requiere que la ejerza el beneficiado por ella, sino que basta que la haya utilizado cualquier persona con el objeto de obtener el consentimiento.

En los contratos electrónicos, se debe distinguir entre la fuerza ejercida contra el titular del código de acceso o de identificación personal, y la que se ejerce sobre un individuo que no sea titular de éste.

Por otro lado, de igual manera como el error podía afectar la formación del programa o su ejecución, la fuerza puede recaer tanto sobre el creador o sobre el ejecutor de dicho programa. En las dos situaciones se vicia el consentimiento debido a que ambas “son manifestación de la voluntad contractual”.¹³⁰

4.1.7.3. Dolo.

Según el Código Civil, el dolo para viciar la voluntad debe ser obra de una de las partes y aparecer claramente que sin él no se hubiera contratado.¹³¹ En los demás casos, sólo da lugar a la acción de perjuicios en contra de quien lo ha fraguado o se ha aprovechado de él.¹³²

En los contratos electrónicos las maquinaciones que una parte utilice para hacer contratar a la otra, pueden ser ajenas al programa. Sin embargo, podrían manifestarse en manipulaciones de la información de dicho programa, tanto en su creación, como con posterioridad.¹³³

¹²⁸ Código Civil, artículo 1456 inciso 1.

¹²⁹ Código Civil, artículo 1456 inciso.

¹³⁰ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 21.

¹³¹ Código Civil, artículo 1458 inciso 1.

¹³² Código Civil, artículo 1458 inciso 2.

¹³³ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 21.

En todo caso, cualquiera sea el método empleado por el contratante doloso para inferir injuria, las consecuencias serán las indicadas en el Código Civil.

4.2. Capacidad.

En los contratos celebrados por medios electrónicos, rigen las mismas normas del derecho civil en materia de capacidad.

Así, si un absolutamente incapaz celebra un contrato electrónico, el acto adolece de nulidad absoluta (o de inexistencia para parte de la doctrina). Si el contrato lo celebra un relativamente incapaz, adolece de nulidad relativa.¹³⁴ Sin embargo, si estos contratantes incapaces cumplen con las formalidades habilitantes que establece la ley, sus actos son plenamente válidos.

Los contratantes deben tener capacidad al momento de celebrar el contrato. Ahora bien, si el medio a utilizar es el computador, también deberán tenerla *al tiempo de admitir que el acto se celebrará por medios electrónicos, y al expresar su voluntad potencial* (es decir, al elaborar el programa computacional).¹³⁵

Es interesante tener presente que los proveedores de servicios a través de Internet difícilmente pueden estar seguros de que el usuario que se comunica con ellos es una persona capaz. Por ejemplo, en el caso de un menor que accede a un servicio de compraventa de bienes utilizando la tarjeta de crédito de su padre. El contrato celebrado por el menor, ¿será nulo? Al parecer, en virtud de la teoría de las apariencias, el titular de la tarjeta queda obligado por el contrato firmado por aquel incapaz.

Otro problema importante surge a propósito de la *representación*. Puede suceder que un individuo actúe en nombre de una persona, teniendo poder para ello y conociendo el código o clave de acceso necesario para contratar. En este caso, la contratación es perfecta y vincula a la persona en nombre de quien se ha contratado.

Sin embargo, sería conveniente que para actuar representando a otro, se hiciera uso de una clave diversa a la del representado, con el objeto de que la contraparte tome conocimiento de que se está contratando a través de un representante.

¹³⁴ Código Civil, artículo 1682.

¹³⁵ Cfr. con lo señalado a propósito de las etapas de la voluntad, Capítulo I, apartado 4.1.1. de esta memoria.

Por último, es necesario indicar la posibilidad de que el poder que un individuo otorga a otro para contratar, y con él la clave, pueda ser revocado. En esta situación, sería aconsejable una modificación de aquella clave con el objeto de evitar contratos indeseados.¹³⁶

4.3. Objeto.

El uso de medios electrónicos en el perfeccionamiento de esta nueva forma contractual, no modifica los requisitos del objeto. Así, es necesario que éste sea posible y determinado si se trata de un hecho del hombre, y real, comerciable, lícito, determinado o susceptible de determinación, si es una cosa del mundo externo.

Sin embargo, la utilización de estos medios podría dificultar su determinación. Esto se produce en los casos en que se utilizan instrumentos tecnológicos que van más allá de simples nexos de comunicación, como ocurre con los computadores previamente programados (usan el EDI por ejemplo), es decir, que responden a un estímulo, emitiendo la aceptación contractual. Es por esto que la determinación se presenta como un requisito trascendental del objeto de estos contratos, por lo que ha de ser más precisa.¹³⁷

Desde otro punto de vista, es interesante mencionar lo que ocurre en las transacciones electrónicas internacionales. Puede ocurrir que ciertos objetos sean comerciables en algunos países y en otros no. Es lo que ocurre, por ejemplo, en Singapur donde la comercialización de pornografía se encuentra prohibida. Sin embargo a través de Internet, sus habitantes acceden libremente a ella.¹³⁸

¹³⁶ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 14.

¹³⁷ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 22.

¹³⁸ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit., pág. 37.

4.4. Causa.

Como se recordará, la Teoría de la Causa es uno de los temas más complejos y debatidos por la doctrina, llegándose a poner en duda no sólo su ámbito sino incluso su existencia.

Para el Código Civil chileno, la causa es el motivo que induce al acto o contrato.¹³⁹

Es necesario que ésta sea real, por oposición de falsa o a falta de causa. Además, debe ser lícita, es decir, que no esté prohibida por la ley o sea contraria a las buenas costumbres o al orden público.

Este requisito, al igual que el objeto, opera de igual manera en las formas tradicionales de contratación y en los contratos electrónicos por lo que no se entrará en mayor detalle.

4.5. Formalidades.

Es el aspecto más modificado en la contratación electrónica.

El uso de medios electrónicos en el perfeccionamiento de estos contratos provoca que la identificación de la persona con quien se contrata y la autenticidad de los datos que ésta aporta, sean de difícil determinación. De esta forma, el aportar “un documento emitido por un medio electrónico, no asegura quién es la persona que lo ha emitido, cuando menos de una forma indubitada, ni si el contenido del mensaje recibido, coincide con el del emitido.”¹⁴⁰

Es cierto que en materia mercantil, para lograr beneficios económicos, la agilidad en las operaciones es muy importante. Sin embargo, no se debe olvidar la inseguridad que se ocasiona si no se comprueban todos los datos necesarios en un contrato, dado el riesgo que supone llegar a un consentimiento nulo por error.

El uso, por ejemplo, de computadores con acceso a las redes de comunicación, constituye una gran ayuda en la fase precontractual. Sin embargo, en la fase de perfeccionamiento, se requiere de mayores garantías, las que, aunque pudieran retrasar ciertas decisiones, aseguran un tráfico mercantil seguro.

¹³⁹ Código Civil, artículo 1467 inciso segundo.

¹⁴⁰ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 23.

El legislador chileno, consciente de los problemas que se pueden derivar de lo anteriormente señalado, reconoce validez expresa a los actos y contratos suscritos por medio de firma electrónica. Incluso más, les otorga el mismo valor y efectos que los celebrados por escrito y en soporte de papel.¹⁴¹

4.5.1. Posibilidad de dar cumplimiento a las formalidades del Derecho Civil a través de medios electrónicos.

Como se sabe, la ley, atendiendo distintas finalidades, exige el cumplimiento de requisitos externos para determinados actos jurídicos. De aquí la distinción entre formalidades por vía de solemnidad, por vía de habilitación, por vía de prueba y por vía de publicidad.

A simple vista, el ciberespacio no permite la aplicación de estas formalidades exigidas en la contratación tradicional. Sin embargo, con el objeto de llegar a una conclusión propia al respecto, se utilizará la misma distinción señalada anteriormente para determinar si es factible o no cumplir con ellas por la vía electrónica.

En primer lugar, se entenderá por formalidades por vía de solemnidad los requisitos externos indispensables para el perfeccionamiento del acto o contrato.¹⁴²

Es en el derecho de familia donde estas solemnidades encuentran su principal aplicación. Sin embargo, debido a que el comercio electrónico no incluye este tipo de actos, no existe, por el momento, ningún problema.

Las dificultades surgen respecto a los actos patrimoniales. Así, por ejemplo, el artículo 1801 inciso 2 del Código Civil chileno exige que la compraventa de bienes raíces conste por escritura pública.¹⁴³

El legislador ha establecido estas exigencias, con el objeto de que las partes tomen conciencia de la trascendencia y seriedad del acto, evitando decisiones sin una previa reflexión. Por otro lado, pretende que el Estado (a través del notario) certifique la veracidad, otorgando seguridad jurídica a las partes y a los terceros.

¹⁴¹ Artículo 3, Ley 19.799 sobre Documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, publicada en el Diario Oficial el 12 de abril del año 2002.

¹⁴² Moreno Monroy, René, op. cit.

¹⁴³ Otro caso es el otorgamiento de un instrumento privado en la promesa de celebrar un contrato (artículo 1554 del Código Civil).

En la actualidad, no es posible dar cumplimiento a estas solemnidades a través de medios electrónicos. Esto se desprende del artículo 3 letra A de la Ley 19.799, que no considera como válidos los actos o contratos a los que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico.¹⁴⁴

Sin embargo, no es que dicha ley se niegue a la celebración de actos solemnes, sino sólo a aquellos cuyas formalidades no pueden cumplirse por medios electrónicos.

De esta manera, se deja abierta la posibilidad que, a través de una modificación legal, se implementen las Notarías Digitales. Determinadas personas jurídicas pueden encargarse de certificar la veracidad y exactitud de un documento electrónico y, al mismo tiempo, cerciorarse de que el que envía la información es en realidad la persona que dice ser. Todo esto, utilizando los medios de encriptación disponibles en la actualidad, los que serán tratados en el Capítulo III.

Las formalidades por vía de habilitación, son aquellas destinadas a proteger a las personas incapaces, supliendo o completando su capacidad, o reemplazando o complementando una capacidad imperfecta.¹⁴⁵ Ejemplo de éstas es la autorización del representante legal de un incapaz.

Estas formalidades tienen plena aplicación en los contratos electrónicos.

El problema surge respecto a la autorización o ratificación de los representantes legales que, por exigencia del legislador chileno deben constar por escrito, y que se abordarán tangencialmente al tratar el requisito de escriturar.¹⁴⁶

Existe una situación que podría darse en los contratos digitales.

Se trata de la *contratación con un relativamente incapaz*¹⁴⁷ a quien falta la autorización o ratificación de su representante legal. Este contrato genera una obligación natural en virtud del artículo 1470 inciso 4 N° 1 del Código Civil, lo que se traduce en que el acreedor no puede exigir el cumplimiento del contrato, salvo que el deudor se obligue en su peculio profesional.

Debido a esto, el oferente debe asegurarse que quien adquiere sus productos y servicios tiene la capacidad suficiente para contratar. Sin embargo, esto resulta bastante más difícil en la contratación por medios electrónicos.

¹⁴⁴ Además, en las letras B y C excluye a aquellos actos en que la ley requiera la concurrencia personal de alguna de las partes y aquellos relativos al derecho de familia.

¹⁴⁵ Moreno Monroy, René, op. cit.

¹⁴⁶ Cfr. Capítulo I, 4.5.2.

¹⁴⁷ Caso del menor adulto y del disipador interdicto, según el artículo 1447 inciso 3 del Código Civil.

En la mayoría de los sitios de venta por Internet se exige el uso de una tarjeta de crédito como medio válido para el pago. De este modo, existe mayor certeza de que quien está contratando es una persona capaz. Así, si tiene a su disposición una tarjeta de crédito, es porque ha sido autorizada por el banco para realizar la transferencia, por lo que se trata de una persona capaz, o que actúa dentro de su peculio profesional, o, por lo menos, ha sido autorizado por su representante para obtener la tarjeta o efectuar la transacción.

Las formalidades por vía de publicidad, son aquellas que tienen por objeto permitir que quienes no han intervenido en la celebración de un acto jurídico tomen conocimiento de su realización.¹⁴⁸

Cuando estas formalidades consisten en la *inscripción en un registro público*, aparece la duda respecto a la forma de darles cumplimiento por la vía electrónica.

Sin embargo, técnicamente, es perfectamente posible sugerir el acceso a las bases de datos de dichos registros a través de la red. De esta manera, se podrían efectuar todos los trámites en línea, con la participación de las partes, del notario electrónico y del registro, simplificando en gran medida los trámites de este tipo.

Es necesaria una modificación legal, con el objeto de implementar esta alternativa.

Por último, las formalidades por vía de prueba, son aquellas que tienen por objeto acreditar la celebración de un acto jurídico.¹⁴⁹

Hay casos en que el legislador exige escriturar y/o firmar un acto o contrato para dar cumplimiento a esta formalidad.¹⁵⁰ Por ejemplo, la exigencia del legislador chileno, como formalidad por vía de prueba, que consten “por escrito los actos y contratos que contengan la entrega o promesa de una cosa que valga más de dos unidades tributarias.”¹⁵¹

A primera vista, parece difícil dar cumplimiento a esta exigencia de la ley por la vía electrónica. Sin embargo, para llegar a una conclusión, se procederá a tratar los requisitos de escriturar y firmar en forma genérica, es decir, cuando la ley los exige para dar cumplimiento a cualquier clase de formalidad.

¹⁴⁸ Moreno Monroy, René, op. cit.

¹⁴⁹ Ibid.

¹⁵⁰ No se debe olvidar que la escrituración y firma también puede ser una formalidad por vía de solemnidad o, incluso, por vía de habilitación.

¹⁵¹ Código Civil, artículo 1709.

4.5.2. Requisito de escriturar.

¿Qué entiende el Código Civil por “constar por escrito”?

El *Diccionario de la Lengua Española* define “por escrito” como hecho “por medio de la escritura”.¹⁵² A su vez, conceptualiza el vocablo “escribir” como “representar las palabras o las ideas con letras u otros signos trazados en papel u otra superficie, por medio de pluma y tinta o de otro instrumento adecuado a este fin, o por medio de la mecanografía.”¹⁵³

En sentido literal, los contratos electrónicos no cumplen con este requisito de la escritura. Sin embargo, es conveniente atender a las razones que tuvo la ley para requerir de ella en ciertos actos y contratos.

Así, se pueden mencionar las siguientes motivaciones del legislador:

- 1) Dejar constancia, de manera tangible, de la existencia y naturaleza de las intenciones de las partes para obligarse mutuamente.
- 2) Facilitar a las partes el conocimiento de todas las obligaciones derivadas del contrato, garantizando que el documento sea legible por cualquier persona.
- 3) Asegurar que el documento se conserve inmodificable, dejando evidencia de la transacción.
- 4) Permitir la reproducción del documento, quedando ambos contratantes con la misma información.
- 5) Conservar la información de un modo concreto: en el escrito.
- 6) Simplificar el control y las auditorías derivadas del acto o contrato sea por razones tributarias, de contabilidad u otras.

Como se puede observar, los contratos electrónicos cumplen de mejor manera estos objetivos. Así, no hay duda de que crean una evidencia tangible de las intenciones de las partes, del mismo modo como lo haría un contrato tradicional. Por otro lado, agilizan e incluso mejoran el conocimiento de las obligaciones generadas, y permiten en forma más sencilla la copia del documento. Además, a través de los actuales medios de encriptación, la inviolabilidad del documento está asegurada. Por último, el documento

¹⁵² Real Academia Española, *Diccionario de la Lengua Española*, Decimonovena Edición, Editorial Espasa-Calpe, Madrid, 1970, pág. 562.

¹⁵³ Ibid.

electrónico puede ser conservado, archivado y organizado de manera eficiente, sin ocupar grandes espacios físicos, lo que simplifica el control y demás auditorías.

El legislador, consciente de todo ello, estableció en el artículo 3 de la *Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma* que los actos y contratos suscritos por medio de firma electrónica “se reputarán como escritos, en los casos en que la ley exija que los mismos consten de este modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.”

4.5.3. La firma.

El legislador impone este requisito con el objeto de:

- 1) Identificar a las personas y asegurar su implicancia personal en el acto, sea como autor o testigo.
- 2) Garantizar la presencia de un individuo en un momento y lugar determinado.
- 3) Demostrar la intención de obligarse por el contenido del documento.

En la actualidad la tecnología ha creado las *firmas digitales*, por medio de las cuales es posible atribuir la autoría de un documento a cierta persona. A través de éstas se asegura que un individuo previamente determinado, es el autor de un documento.

Estos sistemas funcionan mediante claves que los computadores comparan con llaves digitales, garantizando con precisión matemática, que la persona que dice que emitió el documento es la misma. Además, aseguran que el documento no ha sido modificado con posterioridad, vale decir, después de haberse emitido.¹⁵⁴

La firma digital mejora la seguridad que brinda la firma manuscrita, por lo que se cumplen con creces las finalidades de este requisito. Así lo ha entendido la *Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma*, la que en su artículo 3 inciso tercero, establece que “la firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales(...)”.

¹⁵⁴ Cfr. Capítulo III, apartado 4.

5. Fases de la contratación electrónica.

Una vez que las partes toman la decisión de contratar por medios electrónicos, el contrato que se perfecciona a través de estos medios, tiene una serie de fases, que vienen a coincidir con las etapas del contrato ordinario.

Así, se distinguen tres etapas:

- Fase de generación o precontrato.
- Fase de perfeccionamiento del contrato.
- Fase de conclusión o consumación del contrato.

5.1. Fase de generación o precontrato.

Esta primera etapa se refiere a toda la actividad en relación al examen de las posibilidades de contratar. El futuro aceptante estudia en forma detallada la oferta, tanto respecto a las características del objeto como también a todas las condiciones y cláusulas del futuro contrato. Ambas partes examinan las ventajas y desventajas de la negociación en concreto.

El uso del computador en este período puede abarcar distintos aspectos. El ordenador puede *atender a impulsos externos*, si previamente ha sido programado para eso, aceptando o rechazando una oferta. También puede ser el *origen* de una oferta. En la mayoría de los casos, es sólo un medio de comunicación, esto es, un *simple nexa* entre oferente y aceptante.

Ahora bien, si “(...) le concedemos cierto carácter “decisorio”, no es que tenga la posibilidad de decidir, *stricto sensu*, sino que el ordenador en cuyo programa se hayan introducido una serie de exigencias para emitir la aceptación, lo único que podrá hacer, en esta primera fase de generación será emitir su disconformidad por no reunir los requisitos almacenados”.¹⁵⁵

De lo anterior se puede deducir que las discusiones propias de la fase precontractual no pueden ser efectuadas por el computador, por lo que se trata de una *etapa predominantemente humana*.

El hombre analizará las ventajas y desventajas que se derivan de un contrato determinado. Podrá utilizar los más variados medios tecnológicos, incluidos el

¹⁵⁵ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 28.

computador, con el objeto de comunicarse, los que en esta situación actuarán como simples *enlaces o nexos* entre las partes.

Toda la información que reciban los contratantes en este período, deberá ser confirmada, a fin de evitar posibles intromisiones que pudieran distorsionar la información en el futuro perfeccionamiento del contrato.

En este punto resulta conveniente emplear alguna de las medidas de seguridad, que serán estudiadas en detalle en el Capítulo III. Por ejemplo, se pueden establecer claves secretas conocidas sólo por los futuros contratantes o cualquier otro medio de autenticación electrónica que pueda ser pactado previamente.

Por todo lo dicho, se puede concluir que esta fase, debido a su naturaleza, requiere del pensamiento y la decisión humana, sin que el computador pueda extenderse a ámbitos fuera de la aceptación o negativa de los datos suministrados por el hombre, esto es, la información introducida en el propio programa.

5.2. Fase de perfeccionamiento.

En esta etapa el computador puede adquirir gran relevancia. A diferencia de lo que sucede en la primera, el ordenador “(...) no sólo puede ser utilizado como medio de comunicación y enlace, pudiendo perfeccionarse el contrato mediante la pulsación del “*enter*”, previo el cumplimiento de una serie de garantías de seguridad (...)”.¹⁵⁶

No existe inconveniente, al menos desde un punto de vista teórico, para que los contratos *se perfeccionen mediante la comunicación entre computadores*, esto es, utilizando programas que emitan ofertas y aceptaciones. De este modo, la intervención humana no irá más allá de la elaboración de los programas.

Esta fase también requiere de la utilización de las garantías y claves de seguridad con el objeto de evitar el posible incumplimiento de una de las partes, así como también la intromisión de un tercero ajeno a la contratación.

¹⁵⁶ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 28.

5.3. Conclusión o pago.

Perfecto el contrato por haber coincidido oferta y aceptación, se pasa a esta etapa, llamada también de ejecución, en la que *han de realizarse las prestaciones derivadas del acuerdo*.

Los efectos de los contratos electrónicos pueden ser comunes a todo contrato y especiales (es decir, con características propias según su clase), lo que dependerá de su naturaleza y contenido.

Los contratos, cualquiera que sea el medio utilizado para su perfección, son obligatorios para las partes que concurren a su celebración y las obligaciones que surgen de ellos tienen la fuerza de una ley para los contratantes, tal como lo dice el artículo 1545 del Código Civil¹⁵⁷ (principio de la fuerza obligatoria del contrato y principio del efecto relativo del contrato).

5.3.1. Forma de dar cumplimiento a las obligaciones.

Con el objeto de evitar razonamientos ajenos a este trabajo, se identificarán y utilizarán como sinónimos los términos cumplimiento y pago de la obligación, a pesar de que jurídicamente, no son absolutamente equiparables.¹⁵⁸

Gran relevancia han adquirido en la actualidad el desarrollo de nuevas formas de cumplir las obligaciones, como el *pago electrónico*, definido como aquel realizado por medios electrónicos¹⁵⁹, y que se verifica en general, mediante una Transferencia Electrónica de Fondos.

¹⁵⁷ El artículo 1545 del Código Civil señala que “Todo contrato legalmente celebrado es una ley para los contratantes, y no puede ser invalidado, sino por su consentimiento mutuo o por causas legales”.

¹⁵⁸ Parte de la doctrina distingue entre cumplimiento normal y anormal de las obligaciones, reservando la palabra pago sólo para el primero de ellos. Otros le dan una acepción amplia, identificándolo con cualquier forma de cumplimiento, sea voluntario o forzoso.

¹⁵⁹ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 41.

5.3.2. El dinero electrónico o virtual.

El dinero, en general, cumple diversas funciones. Tiene una función de depósito, sirve para medir el valor de las cosas y, como instrumento de intercambio y pago.

Ahora bien, el *dinero electrónico*, es “un instrumento de pago reflejado en un soporte informático y que a través de las transferencias electrónicas de fondos, persigue la misma finalidad que el dinero tradicional, dependiendo la efectividad del mismo (,) de su realización”.¹⁶⁰

Los conceptos de *dinero virtual* y *Transferencias Electrónicas de Fondos* (T.E.F.) están íntimamente unidos, ya que éstas suponen exclusivamente el instrumento de movilidad de aquél. El dinero electrónico, para que sea tal y tenga verídica utilidad económica, requiere comunicarse a través de dichas transferencias, poniéndolas de manifiesto a éstas como formas de cumplimiento de las obligaciones. De esta manera, las T.E.F. coincidirían con el pago y el dinero electrónico con el dinero tradicional.¹⁶¹

El pago en Internet realizado a través de mecanismos como cheques, órdenes de pago, giros, etc. o utilizando el teléfono, el correo u otros medios fuera de la red, convierten el procedimiento en lento, caro, inapropiado e incómodo, debido al consumo de innumerables recursos y al ejercicio de operaciones externas a la red.¹⁶² Estos mismos pagos se pueden efectuar dentro de Internet a través de herramientas y servicios que les son propios.

5.3.3. Las Transferencias Electrónicas de Fondos (T.E.F.).

5.3.3.1. Concepto.

Las T.E.F. son operaciones que consisten en un traspaso de fondos de una cuenta a otra para realizar pagos, sin desplazamiento real de dinero.

La transferencia de fondos se inicia a través de “un terminal electrónico, instrumento telefónico, o un computador, o una cinta magnética, a fin de ordenar, dar

¹⁶⁰ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 34.

¹⁶¹ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 35.

¹⁶² Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág.35.

instrucciones o autorizar a una institución financiera, para que adeude o acepte pagos en cuenta.”¹⁶³

Este sistema, no modifica la base del servicio bancario de la transferencia de fondos. Sólo cambia la forma de efectuarlo.

A consecuencia de su uso, el banco aumenta su productividad, disminuye sus gastos en personal y mejora su servicio. Sin embargo, el dinero permanece menos tiempo en la entidad bancaria debido a que los cargos y abonos son prácticamente instantáneos.

5.3.3.2. Formas que pueden revestir las T.E.F.

Las T.E.F. pueden adoptar diversas modalidades. Algunas de ellas se basan en reproducir sobre Internet procedimientos de pago habituales en el comercio tradicional, como por ejemplo el pago con tarjeta de crédito. Otras, como los sistemas que utilizan dinero electrónico, significan cambios más profundos en la actividad comercial.

A continuación se tratarán algunas de ellas, efectuando especial énfasis en las tarjetas magnéticas, que constituyen, en la actualidad, el medio de pago más aceptado por los usuarios de Internet.

1) Dinero efectivo electrónico.¹⁶⁴

Fue creado por David Chaum, a mediados de los noventa, con el objeto de mejorar los medios de pagos a través de redes, fundamentalmente Internet.¹⁶⁵

Para su utilización, el usuario debe instalar un software en su computador, generalmente llamado “wallet” que le permite acceder a un tercero (que actúa como intermediario), para convertir dinero de su cuenta bancaria en dinero virtual, con el que podrá adquirir los bienes deseados.

Por su parte, el comerciante o vendedor, reintegrará este dinero electrónico a cambio de una acreditación en su cuenta bancaria.

Técnicamente, el proceso se lleva a cabo mediante el intercambio de mensajes entre los dispositivos del usuario y del prestador del servicio a través de la red.

¹⁶³ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 37.

¹⁶⁴ También se le ha denominado *e-money* o *electronic money*.

¹⁶⁵ Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, op. cit., pág.24.

Para utilizar este sistema deben pactarse diversos negocios jurídicos entre el usuario y su intermediario, así como también entre el banco o entidad financiera y el intermediario, con el objeto de regular las obligaciones y derechos entre éstos. Además se deben convenir las condiciones de uso del programa, detallando las actividades autorizadas.¹⁶⁶

Los pagos efectuados a través de este instrumento mantienen el anonimato del pagador, lo que se constituye en su principal ventaja. Sus datos no circularán constantemente por Internet, asegurándose su intimidad.

Ejemplo de esta clase de servicio es *CyberCash*.¹⁶⁷

2) Medios para micropagos.

Todo mecanismo de pago tiene un costo que asume, de alguna manera, el comerciante y el comprador, encareciéndose la operación. Por esto, muchas veces no son adecuados para cancelar pequeñas sumas de dinero, de monto inferior al cargo fijo mínimo exigido para las transacciones electrónicas por la mayoría de los sistemas.

Este problema se resuelve mediante los medios para micropagos, los que a cambio de una comisión sobre la cantidad pagada, permiten efectuar transacciones de escasa significación económica. Ejemplo de ello es el servicio dado por *step2u*.¹⁶⁸

3) Cheques electrónicos (*e-check*).

El proveedor del servicio se obliga a transferir al comerciante el dinero que el consumidor pague utilizando este mecanismo, o a servir de nexo con el banco del consumidor para tramitar dicha transferencia.¹⁶⁹

Así, por ejemplo, *CyberCash*, ofrece el sistema de cheques llamado "*PayNow*", a través del cual los proveedores permiten que sus clientes paguen sus cuentas utilizando la Internet.

4) Banca Hogareña (*Home Banking*).

Este producto da la posibilidad al cliente bancario de efectuar traspasos de fondos por vía electrónica desde su domicilio. Además, le permite consultar saldos, ordenar pagos, etc.

¹⁶⁶ Ramos Suárez, Fernando, "Problemas jurídicos de Comercio Electrónico", op. cit., apartado II, F.

¹⁶⁷ Ver www.cybercash.com.

¹⁶⁸ En <http://micropagos.step2u.com>.

¹⁶⁹ Millé, Antonio, "Impacto del Comercio Electrónico sobre la Propiedad Intelectual", op. cit., pág. 347.

5) Tarjetas magnéticas.

Los sistemas de tarjetas magnéticas en Internet funcionan de forma muy similar a como lo hacen en el comercio tradicional. El cliente, usa su tarjeta de crédito, débito o de cliente para comprar productos en una tienda virtual.

Con el objeto de asegurar y autenticar las operaciones, las empresas de tarjetas de compra utilizan especificaciones y estándares de encriptación, como SSL (Secure Sockets Layer), y SET (Secure Electronic Transaction).¹⁷⁰

5.1) El contrato de tarjeta.

Desde el punto de vista del cumplimiento de las obligaciones la tarjeta es “aquel documento mercantil, instrumental y electrónico, que permite a su titular, mediante compromiso contractual con el emisor, servir como documento de pago, a la vez que beneficiarse de una línea de crédito limitada, que podrá utilizar en la compra de bienes o servicios, en establecimientos adheridos al sistema, o en el acceso a cantidades limitadas de dinero en bancos o entidades financieras que hayan concertado el servicio.”¹⁷¹

Entre las características del contrato de tarjeta se pueden señalar que es un contrato de adhesión, ya que está sometido a condiciones establecidas por la entidad prestadora del servicio. Por otro lado, constituye un contrato bilateral, debido a que genera obligaciones para ambas partes.

Además, como nuevo medio de pago, exige una *contratación previa*. En ella intervienen necesariamente, el emisor de la tarjeta, el titular de la misma y el establecimiento unido al sistema.

Es *emisor de la tarjeta*, aquella persona que dentro del marco de su actividad profesional, pone a disposición de su cliente un instrumento de pago, en virtud de un contrato suscrito con él.

¹⁷⁰ SET, corresponde a la sigla inglesa de Transacciones Electrónicas Seguras. Es un protocolo de seguridad utilizado por *Visa* y *Mastercard*, y desarrollado con la colaboración de *Microsoft*, *IBM*, y otras empresas del área tecnológica, que opera mediante técnicas de encriptación y firmas digitales (las que serán tratadas en el Capítulo III de este trabajo), con el objeto de garantizar la identidad de los participantes en la transacción, así como también la confidencialidad e integridad de los mensajes. Además, a diferencia de lo que ocurre con el SSL, soluciona el problema del repudio de la compra. Otero Alvarado, Jorge y Lanckenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit., pág. 49.

¹⁷¹ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 44.

El *titular*, es la persona que dispone de la misma para utilizarla de acuerdo con las condiciones y límites establecidos en el contrato con el emisor.

Los *establecimientos adheridos al sistema* permiten que los instrumentos de pago sean utilizados para las operaciones mencionadas.

El contrato a priori que exige el uso de la tarjeta, ha de ser, por un lado, entre el emisor y el titular, y por otro, entre el establecimiento y el emisor.

Entre las principales obligaciones de las partes en los dos contratos señalados, se pueden mencionar:¹⁷²

1. En el contrato entre emisor y usuario.

- Las obligaciones del emisor de la tarjeta: determinar claramente los gastos que pagará el titular; entregar la tarjeta; otorgar una línea de crédito (en el caso de las tarjetas de crédito); pagar y disponer de dinero efectivo cuando se haga uso de la tarjeta; enviar información periódica al titular; mantener la confidencialidad.

- Las obligaciones del usuario: cancelar las cuotas de emisión y mantenimiento, devolver los montos dispuestos en la línea de crédito; utilizar las tarjetas de acuerdo a lo pactado; cooperar en la seguridad del sistema; e informar al emisor el extravío, robo o modificación de datos.

2. En el contrato entre el emisor y el establecimiento unido al sistema.

- Las obligaciones del emisor: pagar al establecimiento, en conformidad a lo acordado, los importes según las facturas; dar el soporte técnico necesario.

- Las obligaciones del establecimiento adherido: aceptar la tarjeta como medio idóneo para el pago, siempre que sean válidas y se encuentren vigentes; hacer las comprobaciones requeridas para su correcto uso; aplicar el precio del público en general a los usuario de éstas; conservar los documento que acrediten la venta en la forma y tiempo determinados por la legislación tributaria; respetar los límites máximos autorizados en las tarjetas; colocar en lugares visibles los símbolos de las distintas tarjetas utilizables; comunicar al emisor cualquier modificación en la titularidad o situación patrimonial del establecimiento; configurar un registro de las operaciones efectuadas.

¹⁷² Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 45.

5.2) Clasificación de las tarjetas utilizables en el pago electrónico.

Las tarjetas magnéticas, pueden clasificarse según su estructura y forma de pago.

1. Atendida su estructura:

a) Tarjetas anónimas.

Se trata del caso en que se utiliza la organización de los sistemas de tarjetas de crédito¹⁷³ y pago existentes, proponiendo alternativas para aceptar cargos por medios electrónicos a través de intercambios de mensajes seguros, los que evitan que terceros conozcan detalles de la cuenta del consumidor.¹⁷⁴

El usuario dará al comerciante una serie de datos, entre los que se encuentra su nombre, número de tarjeta y fecha de expiración. El comerciante, a su vez, autorizará la transacción si cumple con los requisitos establecidos para ello.

En la página correspondiente, al igual que en las tiendas tradicionales, se señalará si se acepta esta clase de tarjetas como medio de pago.

b) Tarjetas inteligentes (*o smart cards*).

A diferencia de los otros sistemas de pago y de las tarjetas anteriormente señaladas, éstas no sólo se basan en recursos de software. Éstas poseen en su interior un chip que contiene un sistema operativo y aplicaciones de software, los que son insertados en su proceso de fabricación.

Su adquisición se realiza de diversas formas dependiendo del producto. En ciertos casos pueden ser compradas anónimamente en máquinas expendedoras (caso de las tarjetas telefónicas prepagadas, por ejemplo), o, utilizando tarjetas de crédito o débito. A veces, también involucran una cuenta bancaria del usuario.

Para recargar la tarjeta con unidades de valor, el usuario del servicio puede utilizar cajeros automáticos, computadores o, incluso, la vía telefónica.

La entidad operadora provee a los comerciantes de terminales u otros dispositivos que permiten realizar transacciones.

¹⁷³ Entre las tarjetas de crédito más utilizadas en la actualidad se encuentra Visa, Mastercard, American Express, Dinners.

¹⁷⁴ Millé, Antonio, "Impacto del Comercio Electrónico sobre la Propiedad Intelectual", op. cit., pág. 347.

En algunas ocasiones, como ya se indicó, involucran una cuenta bancaria perteneciente al usuario. En estos casos para efectuar una compra, el usuario introduce la tarjeta en la terminal e ingresa su clave y la suma a pagar. La terminal, por su parte, verifica que el balance que surge de la tarjeta permita realizar la operación e instruye para que se debite la suma a pagar. Luego la tarjeta ordena a la terminal del vendedor que incremente su balance en la misma suma.¹⁷⁵

Como ejemplo, de esta clase de tarjetas se puede mencionar a *Mondex*, un producto del *Hong Kong & Shanghai Bank Corporation*, muy extendido en países como Inglaterra, donde se utiliza para compras pequeñas.¹⁷⁶

2. Según la forma de pago:

a) Tarjetas de crédito.

Éstas otorgan a su titular la posibilidad de beneficiarse de una línea de crédito, por lo que se pueden adquirir bienes y servicios hasta el límite establecido al contratarla.

b) Tarjetas de compra o de clientes.

Son aquellas que provienen de una firma comercial (tiendas por departamentos, supermercados, etc.). Se caracterizan porque el comerciante ante el cual se utiliza es al mismo tiempo el emisor de ella y quien otorga el crédito.

Es importante señalar que son un tipo de tarjeta de crédito, sin embargo generalmente, no pueden ser utilizadas para pagar en un establecimiento distinto al que la emitió.

c) Tarjetas de débito.

Otorgan acceso a la cuenta corriente de su poseedor, en la que se representarán casi inmediatamente las transacciones efectuadas mediante su uso.

¹⁷⁵ Devoto, Mauricio y Lynch, Horacio M., “Banca, comercio, moneda electrónica y la firma digital”. *Revista de Derecho Informático (REDI)*, No.2, Septiembre 1998 (c1998-2003, Alfa Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/3-3.asp> , apartado 3.3.

¹⁷⁶ Millé, Antonio, “Impacto del Comercio Electrónico sobre la Propiedad Intelectual”, op. cit., pág. 348.

6. La interpretación contractual.

6.1. La interpretación en el Código Civil.

El Código Civil chileno establece, entre los artículos 1560 y 1566, una serie de normas relativas a la interpretación de los contratos. Estos principios reconocidos por el legislador para la contratación clásica, son aplicables a los contratos perfeccionados de manera digital.

El mismo cuerpo legal, en materia de interpretación, sigue la doctrina subjetivista¹⁷⁷¹⁷⁸, es decir, hace primar la voluntad real por sobre la declarada, por lo que considera que la interpretación contractual “se debe reducir a pretender descubrir la intención de las partes”.¹⁷⁹

Sin embargo los contratos electrónicos, en ocasiones, suponen la utilización de “un lenguaje, en cierto modo estereotipado, con expresiones a las que el comercio y la técnica, dan un significado determinado, no pudiéndose alegar una interpretación particular, cuando menos sin una muy fundada justificación”.¹⁸⁰

Ello es aplicable a los contratos en que el computador sirve de nexo a las partes, y con mayor razón, a los celebrados entre computadores preprogramados (contratación vía EDI), debido a que el ordenador responderá al sentido que previamente tenga en su programa. En consecuencia, no es posible admitir un subjetivismo del que carecen tales contratos.

¹⁷⁷ Para la interpretación de los contratos existen, fundamentalmente, dos sistemas. El subjetivo (seguido por los Códigos influenciados por el Código Civil francés e italiano), da primacía a la voluntad real de las partes. El sistema objetivo (para los inspirados en el Código alemán), otorga preeminencia a la voluntad declarada o manifestada, por sobre la deseada o querida por los contratantes. Abeliuk Manasevich, René, *Las Obligaciones*, Tomo I, op. cit., pág. 89.

¹⁷⁸ Esto se deduce del artículo 1560 del Código Civil que señala: “Conocida claramente la intención de los contratantes, debe estarse a ella más que a lo literal de las palabras.” Es la misma solución dada para la interpretación de los testamentos (artículo 1069).

¹⁷⁹ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 48.

¹⁸⁰ *Ibid.*

6.2. Variaciones en la interpretación de los contratos.

Los contratos electrónicos, a diferencia de los tradicionales, son interactivos y dinámicos, por lo que la constante creación informativa y la incorporación de situaciones nuevas no previstas al contratar o al formarse el consentimiento, pueden producir cambios en la situación normal de los convenios entre las partes.¹⁸¹

Estos contratos suelen producir y crear información, la que se incorpora en beneficio de las partes hasta que se produce el consentimiento. Así las partes elaboran *un medio susceptible al cambio*, el que difiere completamente de aquel que tiene lugar en los contratos tradicionales, y que incide tanto en la naturaleza de las relaciones entre los interesados, como en la estructura y en la forma de resolver los conflictos.¹⁸²

Los contratos concluidos por medios digitales son verdaderas *fuentes de interpretación* de los mismos, debido a que normalmente, los mensajes que contienen la oferta son abundantes e incluyen las diversas posibilidades de conflicto que pueden generarse. En la mayoría de los casos, “las advertencias que rodean una oferta adquieren sentido solamente al tenor de lo que se ofrece, existiendo códigos programáticos, tablas de presentación de precios, definiciones de situaciones o de datos estructurales del contrato, el cual por definición es normalmente de adhesión, no encontrándose hecha la oferta a persona determinada”.¹⁸³

Según Eugenio Gaete, estos problemas de interpretación pueden solucionarse de tres formas:¹⁸⁴

1. Si las partes *conocen exactamente la composición de la oferta*, vale decir, saben cuáles son las calidades de la cosa sobre las que recae y los requisitos esenciales del contrato propuesto (dependiendo si se trata de una compraventa, permuta, arrendamiento, etc.), la ley debe fijar las modalidades, plazos o condiciones de dicho contrato.

A estas modalidades se debe sumar aquellas propias de los contratos electrónicos, como el *medio* en que se desarrollará (por ejemplo, la aceptación debe ser remitida por medio de correo electrónico dentro de los próximos dos días contados de la fecha

¹⁸¹ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 157.

¹⁸² *Ibid.*

¹⁸³ *Ibid.*

¹⁸⁴ *Ibid.*

señalada) o las *condiciones* en que tendrá lugar el contrato (como que la oferta tendrá lugar siempre que existan bienes en stock al tiempo de aceptarse la oferta).¹⁸⁵

2. Respecto a la *aceptación*, ella deberá producirse mientras esté pendiente la oferta.

Como la oferta normalmente no va dirigida a una persona determinada, no es posible debatir sobre las cláusulas contractuales, por lo que no cabe una aceptación parcial ni condicional.

3. Por último, las *cláusulas de uso común* se entienden incorporadas, según la costumbre del lugar.

En Chile, en esta materia, son aplicables la *Ley 19.496 sobre Protección de los Derechos de los Consumidores*¹⁸⁶ y los artículos 97 al 106 del Código de Comercio.

Además, el artículo 1 inciso 2° y 3° de la *Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma* establece que la interpretación de ella deberá guardar armonía con los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel.

Por último, la *Ley Modelo sobre Comercio Electrónico de UNCITRAL*, indica en su artículo 3, que en su interpretación deberá tomarse en cuenta:

1) Su “origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.”

2) Las cuestiones regidas por la presente ley no resueltas expresamente por ésta, se resolverán de acuerdo “con los principios generales en que ella se inspira”.

7. Los riesgos en la contratación digital.

El problema de los riesgos,¹⁸⁷ es resuelto por la denominada *teoría de los riesgos*, la que pretende determinar qué ocurre con la obligación cuando ésta se ha hecho imposible, sin que la imposibilidad pueda imputarse al deudor.¹⁸⁸

¹⁸⁵ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 158.

¹⁸⁶ Ley 19.496 que establece normas sobre protección de los derechos de los consumidores, publicada en el Diario Oficial el 7 de marzo de 1997.

¹⁸⁷ El riesgo es la “contingencia o proximidad de un daño.” Abeliuk Manasevich, René, *Las Obligaciones*, Tomo II, Tercera Edición, Editorial Jurídica de Chile, Santiago, Chile, 1993, pág. 982.

¹⁸⁸ Abeliuk Manasevich, René, *Las Obligaciones*, op. cit. pág. 983.

Así, si el incumplimiento es por caso fortuito, en los *contratos unilaterales* la obligación de restituir se extingue sin consecuencias posteriores para las partes. El tema adquiere relevancia a propósito de los *contratos bilaterales* (y en los sinalagmáticos imperfectos), en los que la obligación de la contraparte puede subsistir o no, dependiendo si el riesgo es de cargo del deudor o del acreedor. Las diversas legislaciones recurren a alguna de estas dos alternativas.

En el derecho chileno, por ejemplo, en virtud del artículo 1550 del Código Civil,¹⁸⁹ el riesgo en las *obligaciones de dar una especie o cuerpo cierto* es de cargo del acreedor, salvo en cuatro excepciones: 1) cuando el deudor se constituye en mora de entregar la especie o cuerpo cierto; 2) cuando el deudor se ha comprometido a entregar una misma especie a dos o más personas por obligaciones distintas; 3) cuando las partes así lo estipulen; 4) cuando el legislador expresamente señala una solución contraria, como por ejemplo en el arrendamiento (artículo 1950 N° 1) o en la confección de una obra material (artículo 1996). Respecto a las *obligaciones de género, en las que éste es objeto de alguna forma de especificación*, se recurre a las mismas reglas dadas para las cosas específicas (vale decir, el riesgo lo asumiría el acreedor).¹⁹⁰ En las *obligaciones de hacer y no hacer* el riesgo no fue regulado, por lo que la doctrina plantea dos posibles soluciones: 1) aplicar analógicamente el artículo 1550, caso en que el riesgo recaería en el acreedor, o 2) buscar la respuesta en la equidad, que sería colocar el riesgo a cargo del deudor, como en el artículo 1996 a propósito de la confección de una obra material.^{191 192}

Señalados los principios generales, se intentará determinar los riesgos que se generan en los contratos electrónicos.

En general, los riesgos en esta clase de contratos no se refieren a la *cosa objeto del contrato*, ya que ésta continuará regida por las disposiciones establecidas en el Código de Comercio y en el Código Civil. En este caso, se refieren, principalmente, a *los riesgos que se generan a “consecuencia de la interacción en un medio informatizado, y que atentan a la seguridad misma del contrato y de sus cláusulas”*.¹⁹³

¹⁸⁹ El artículo 1550 del Código Civil establece: “El riesgo del cuerpo cierto cuya entrega se deba, es siempre a cargo del acreedor; salvo que el deudor se constituya en mora de efectuarla, o que se haya comprometido a entregar una misma cosa a dos o más personas por obligaciones distintas; en cualquiera de estos casos, será a cargo del deudor el riesgo de la cosa, hasta su entrega”.

¹⁹⁰ El artículo 1821 del Código Civil, a propósito de la compraventa señala que “la pérdida (...) pertenecerá al comprador (acreedor) (...)”.

¹⁹¹ Los artículos 142 y 143 del Código de Comercio regulan los riesgos en la compraventa mercantil.

¹⁹² Abeliuk Manasevich, René, *Las Obligaciones*, Tomo II, op. cit., pág. 993.

¹⁹³ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 160.

En el derecho documental clásico los riesgos son un *elemento del contrato*, y las partes deben asumirlos de acuerdo a las normas ya señaladas. Ahora bien, si en su celebración tuvieren lugar alteraciones o modificaciones a éste, ellas constituirían, desde una perspectiva penal, falsificaciones documentales (públicas o privadas, dependiendo de la naturaleza del documento), y nulidad del acto en el ámbito civil.¹⁹⁴

Sin embargo, en la contratación digital se prescinde del elemento documental tradicional, y se incorpora un nuevo elemento: *el medio utilizado para celebrar el contrato*. Este medio es dinámico e implica la posibilidad de efectuar alteraciones o cambios en la emisión de datos, los que *dejan de ser elementos formales del contrato* (como sucede en el documento tradicional), *para convertirse en integrantes de éste* (sea como elementos esenciales, naturales o accidentales).

Así por ejemplo, una modificación en la tabla de intereses de una compraventa a plazo, repercutirá en cada una de las cuotas. Dichas tablas se incorporan en forma automática al contrato, mediante la base de datos que corresponde a éste, por lo que una variación en éstas no sólo implica una falsificación documental, sino que además produce una alteración en el contrato mismo, en su esencia, naturaleza o modalidades.

En consecuencia, toda la teoría de los riesgos influirá en los contratos electrónicos, por lo que dichos riesgos deben ser incorporados al contrato y no mantenerse ajenos a él, generando efectos civiles de carácter formal.¹⁹⁵ Este es, precisamente, el carácter que asumen los riesgos en la contratación electrónica.

Los riesgos originados en una transmisión de datos pueden ser voluntarios o involuntarios.

1) Riesgos voluntarios. Son aquellos que tienen su origen en el *acto doloso o culposo* de un tercero que interviene los sistemas de redes, modificando los programas o causando un mal funcionamiento, como el extravío de datos, su divulgación no autorizada o la tardanza en la entrega de éstos.

En Chile, esta materia está regulada por la *Ley 19.223 relativa a los delitos informáticos*. Además, son aplicables las disposiciones civiles en materia de indemnización por los perjuicios causados en materia contractual.

2) Riesgos involuntarios. Son los debidos a un caso fortuito y que se traducen en un mal funcionamiento de la red de información.

¹⁹⁴ Ibid.

¹⁹⁵ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 161.

Pueden tener su origen en causas tan diferentes como problemas eléctricos, disfunción en los sistemas del receptor o del emisor, fallas en las bases de datos, etc. Sus efectos también son variados debido a que pueden alterar en forma temporal o perpetua la transmisión de datos, emitirla o recibirla incorrectamente, retardarla, o incluso, ocasionar la pérdida total o parcial de éstos.

Esta clase de riesgos, cuando se deben a un caso fortuito, los asume el receptor.¹⁹⁶

8. Problemas de Derecho Internacional Privado relacionados con los contratos electrónicos.

Una operación de comercio electrónico puede involucrar agentes de procedencia y características diversas, lo que genera importantes interrogantes desde el punto de vista de la legislación y de la jurisdicción aplicable a los contratos.

Así, por ejemplo, ¿qué sucede si una persona domiciliada en Chile, contrata con un comerciante francés cuyo servidor se encuentra en Estados Unidos? ¿La legislación de qué país regirá un posible conflicto entre las partes?

Se trata de los clásicos problemas del Derecho Internacional Privado, comúnmente denominados conflictos de leyes, ya que se cumple con sus dos elementos: la existencia de una relación jurídica y determinadas circunstancias que permiten aplicar varios cuerpos normativos diferentes.

Dicho de otro modo, los acuerdos comerciales logrados por la vía electrónica son también actos jurídicos y, en muchas ocasiones, coinciden en ellos circunstancias que, “dependiendo del punto de vista (o punto de contacto), permitirían aplicar a dichos acuerdos una legislación diversa”.¹⁹⁷

Esta rama del derecho en el ámbito contractual admite un estatuto mixto. Considera que los *requisitos de fondo* del contrato (capacidad, consentimiento, objeto y causa), se determinan por el *estatuto personal*, que afecta al estado de las personas y a su capacidad para proceder en la relación jurídica. Por otro lado, los *requisitos de forma*, es decir, la manifestación externa del acto, se rige por el *estatuto real*, esto es, aquel

¹⁹⁶ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 162.

¹⁹⁷ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit., pág. 65.

relativo a las cosas, determinando su naturaleza y los modos en que éstas pueden ser habidas por el hombre.¹⁹⁸

Con el objeto de dar mayor claridad al tema, y atendido el ordenamiento jurídico chileno, se distinguirá entre contratos electrónicos celebrados en Chile y contratos electrónicos celebrados en el extranjero.

8.1. Contratos celebrados en Chile.

Como se sabe, en virtud de lo establecido en el artículo 14 del Código Civil¹⁹⁹, los contratos celebrados en territorio chileno se rigen por la *ley chilena*.

Sin embargo, se debe tener presente que el artículo 16 inciso 2º²⁰⁰ del mismo cuerpo legal, acepta en materia contractual el *principio de la autonomía* de la voluntad, por lo que las partes pueden pactar que el contrato se sujete, en ciertos aspectos, a la ley extranjera. Lo mismo se reitera en el artículo 113 inciso 2º del Código de Comercio.²⁰¹

8.2. Contratos celebrados en el extranjero.

A propósito de los actos celebrados fuera del territorio nacional, la legislación chilena distingue entre:

- a) Los requisitos de forma de los actos y contratos;
- b) Los requisitos de fondo y sus efectos; y
- c) Los actos relativos a los bienes.

¹⁹⁸ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 164.

¹⁹⁹ El artículo 14 del Código Civil señala: “La ley es obligatoria para todos los habitantes de la República, incluso los extranjeros”.

²⁰⁰ El artículo 16 inciso 2º establece que: “Esta disposición se entenderá sin perjuicio de las estipulaciones contenidas en los contratos otorgados válidamente en país extraño”.

²⁰¹ El artículo 113 inciso 2º señala que: “Así, la entrega y pago, la moneda en que éste deba hacerse, las medidas de toda especie, los recibos y su forma, las responsabilidades que imponen la falta de cumplimiento o el cumplimiento imperfecto o tardío, y cualquiera otro acto relativo a la mera ejecución del contrato deberán arreglarse a las disposiciones de las leyes de la República, a menos que los contratantes hubieren acordado otra cosa”.

a) En las disposiciones relativas a las formas de los actos y contratos, rige el principio *lex locus regit actum*²⁰², consagrado en el artículo 17 del Código Civil, en virtud del cual, la forma de los instrumentos públicos se determina por la ley del país en que han sido otorgados.

Según jurisprudencia de la Corte Suprema, esta norma es de carácter general, por lo que se aplica no sólo a los instrumentos públicos sino que también a toda clase de documentos, incluso a los privados.²⁰³

Se reconocen *dos excepciones* a este principio:

1) Si la ley chilena exige instrumento público probatorio, no valen las escrituras privadas cualquiera sea la fuerza de ellas en el país de otorgamiento (artículo 18 del Código Civil).

2) Los testamentos verbales otorgados en otro país, sin importar el valor que en tal país se les dé (artículo 1.027 de la misma norma).²⁰⁴

b) Respecto a los requisitos internos de los actos y a sus efectos, siguen la ley del país en que han sido otorgados.

Sin embargo, en lo relativo al *estado y capacidad de las personas para ejecutar ciertos actos que hayan de tener efecto en Chile*, los chilenos quedarán sujetos a la ley chilena y los extranjeros al estatuto vigente en su país (artículo 15 del Código Civil).

En relación a los efectos de los contratos otorgados fuera del territorio nacional, para cumplirse en Chile, deberán, necesariamente, arreglarse a las leyes chilenas, según el artículo 16 inciso tercero del Código Civil y 113 del Código de Comercio.²⁰⁵

c) Tratándose de actos relativos a los bienes, como lo dispone el artículo 16 del cuerpo legal ya citado, se aplica el principio *lex rei sitae*, es decir, la ley del lugar donde están ubicados dichos bienes.

²⁰² Se aplica la ley del lugar de celebración del acto.

²⁰³ Sentencia de la Corte Suprema, de 21 de diciembre de 1927. Revista de Derecho y Jurisprudencia, Tomo XXV, 2º parte, sección primera, pág.544; asimismo, Sentencia de la Corte Suprema, de 14 de enero de 1927. Revista de Derecho y Jurisprudencia, Tomo XXV, 2º parte, sección primera, pág.106, citada por Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 165.

²⁰⁴ Ibid.

²⁰⁵ El artículo 113 inciso 1º del Código de Comercio indica: “Todos los actos concernientes a la ejecución de los contratos celebrados en país extranjero y cumplidos en Chile son regidos por la ley chilena, en conformidad a lo que se prescribe en el inciso final del artículo 16 del Código Civil”.

Si los bienes se encuentran en el territorio nacional, quedarán sujetos a las leyes chilenas “aunque sus dueños sean extranjeros y no residan en Chile”.²⁰⁶ Esta norma se entiende “sin perjuicio de las estipulaciones contenidas en los contratos otorgados válidamente en país extraño.”²⁰⁷

Ahora bien, el contrato electrónico, por ser un contrato a distancia, plantea el problema de determinar el lugar de su celebración. Este punto está relacionado con lo dicho a propósito del *momento y lugar de formación del consentimiento*,²⁰⁸ ya que ello determinará la ley a aplicar.²⁰⁹ Conocido el momento y lugar en que se formó el consentimiento, se podrá determinar la ley aplicable en conformidad con las normas expuestas, o de acuerdo al estatuto predominante en el estado donde se ha producido el consentimiento, en conformidad al estatuto escogido.

En este punto, conviene tener en consideración la Escuela Angloamericana, que sostiene un sistema estatutario diverso, basado en la territorialidad de la ley en forma absoluta respecto de los contratos que recaen sobre inmuebles. Así, aplica el *lex rei sitae* respecto a los requisitos internos del acto y a las formas del mismo. El principio *lex locus regit actum* sólo lo considera para los muebles. Lo señalado adquiere importancia cuando se relaciona con las distintas normas dictadas a propósito de la contratación electrónica. Ejemplo de ello es la *Ley de firma electrónica del estado de Utah*²¹⁰, que incorpora el estatuto territorial, otorgando valor solamente a aquellos contratos electrónicos firmados digitalmente conforme a sus disposiciones. Sin aquella exigencia, no tienen valor legal en dicho estado.²¹¹

En Chile, la *Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*, en el artículo 3 inciso primero, reconoce validez a los actos y contratos suscritos por medio de firma digital. Nada dice sobre el estatuto aplicable a dichos contratos, por lo que se debe recurrir, en esta materia, a las normas del Código Civil y del Código de Comercio señaladas anteriormente, y que establecen el *lex locus regit actum*.

²⁰⁶ Código Civil artículo 16 inciso 1.

²⁰⁷ Código Civil artículo 16 inciso 2.

²⁰⁸ Cfr. Capítulo I, apartado 4.1.4. y 4.1.5. de este trabajo.

²⁰⁹ En virtud del artículo 104 del Código de Comercio chileno, el contrato en que los interesados residan en lugares diversos se entiende celebrado en el lugar de residencia del que hubiere aceptado la propuesta definitiva o la modificada posterior.

²¹⁰ *Digital Signature Act*, Utah, del 1 de mayo de 1995.

²¹¹ *Utah Code, Digital Signature Act*, 46-3-102, 46-3-103, 46-3-201, citado por Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 167.

8.3. Competencia jurisdiccional.

El tribunal competente es determinado por la ley aplicable, por lo que salvo acuerdo de las partes en cuanto a prorrogar la jurisdicción, conocerá del asunto *aquél del estado cuya ley se aplique al contrato electrónico*.

Esto debe entenderse sin perjuicio de las normas sobre competencia propias de cada país en particular, y además, de las sustracciones que las partes de común acuerdo hagan de la justicia ordinaria a la jurisdicción arbitral, nacional o internacional.²¹²

Los contratos de adhesión generalmente recurren al arbitraje como medio de solución de controversias. Incluso algunos postulan la intervención de grupos de expertos antes de recurrir a los árbitros, con el objeto de evitar costosos y lentos procedimientos. Se pretende resolver el problema de manera amistosa entre las partes, a través de la mediación de entendidos en la materia.²¹³

Respecto al arbitraje internacional, el profesor Eugenio Gaete²¹⁴ señala ciertas restricciones importantes de tener en cuenta:

a) La *Convención sobre Reconocimiento y Ejecución de Sentencias Arbitrales Extranjeras*²¹⁵, en su artículo V N° 2, permite denegarle reconocimiento y ejecución a una sentencia arbitral internacional si la autoridad del país en que se solicita tal reconocimiento y ejecución acredita que tal cuestión no es susceptible de arbitraje de conformidad con su ley nacional, o que el reconocimiento y ejecución atentan contra el orden público interno de ese país.

b) Para que se verifique el arbitraje internacional, es necesario que se trate de un contrato a distancia, que puede o no ser electrónico, de individuos que tengan domicilio en naciones diferentes. Sólo de esta manera podrá conocerlo un tribunal arbitral internacional.

²¹² Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 167.

²¹³ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit., pág. 64.

²¹⁴ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 168.

²¹⁵ Naciones Unidas, *Convención sobre Reconocimiento y Ejecución de Sentencias Arbitrales Extranjeras*, Nueva York, 10 de junio de 1958.

c) De acuerdo a la *Ley Tipo sobre Arbitraje Comercial Internacional de la UNCITRAL*²¹⁶, es necesario que el contrato contenga una *cláusula que permita someter* el litigio existente a un tribunal arbitral internacional.

d) Debe tratarse de un acto de comercio, situación de hecho que determinará el tribunal.

e) El tribunal deberá decidir sobre el derecho aplicable al caso particular. Si esto no se realizara, el tribunal tendrá que “aplicar la ley designada por la norma en conflicto de leyes que juzgue aplicable para el caso”.²¹⁷

8.4. Posible solución.

Es necesario un replanteamiento de los problemas relativos al Derecho Internacional Privado, en el sentido de poder determinar la ley aplicable y, consecuentemente, el tribunal que conocerá de los posibles conflictos a que den origen los contratos electrónicos.

La adopción de un *tratado internacional* en el que se estipule un principio general parece una buena medida. Así, se podría determinar la legislación aplicable a las operaciones realizadas en el ciberespacio y el tribunal competente para conocer de los litigios. Ello, obviamente, sin perjuicio de que las partes puedan someterse expresa y voluntariamente a algún determinado ordenamiento legal.

Incluso, es posible utilizar los tratados vigentes hoy en día para las transacciones comerciales internacionales, lo que evitaría una discriminación entre los diferentes medios para contratar.²¹⁸

²¹⁶ UNCITRAL, Comisión de Naciones Unidas para el Derecho Mercantil Internacional, Ley Tipo de Arbitraje Comercial Internacional, del 21 de Junio de 1985.

²¹⁷ Artículos 23, 24, 25 y 28 de la Ley Tipo de Arbitraje Comercial Internacional, citada por Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 168.

²¹⁸ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit., pág. 65.

8.4.1. Convenios Internacionales aplicables al contrato celebrado mediante la Internet.

En la actualidad se está lejos de alcanzar un marco jurídico internacional de carácter universal. Sólo existe una multitud de normas aplicables al contrato vía Internet, donde los contenidos son bien diferentes: ley del vendedor, leyes de los compradores, o un conjunto de disposiciones aplicables a las normas de conflictos.

A continuación se indicarán algunas de ellas, con el propósito de conocer las distintas formas de abordar este problema que tiene hoy el derecho internacional.

Existen convenciones que regulan específicamente la compraventa internacional. En este ámbito, se encuentra la Convención de Naciones Unidas del 11 de Abril de 1980, llamada *Convención de Viena sobre la Compraventa Internacional de Mercaderías*. Entró a regir el 1 de Enero de 1988 y se encuentra ratificada por cerca de cincuenta estados pertenecientes a sistemas jurídicos tan diversos como Francia, Estados Unidos, China, y Chile.

Esta Convención adquiere gran trascendencia debido a que otorga normas uniformes para los países firmantes, permitiendo la ejecución de los contratos celebrados entre vendedores y compradores de los estados que la han ratificado, reduciendo los conflictos entre los distintos sistemas jurídicos.

Su ámbito de aplicación está delimitado a los contratos de compraventa de mercaderías entre partes establecidas en países diferentes, cuando aquellos estados sean países firmantes, o cuando las reglas de derecho internacional privado conduzcan a la aplicación de la Ley de un estado contratante.²¹⁹

La Convención sólo regula la formación y las obligaciones nacidas del contrato de venta, excluyendo las normas sobre validez de los contratos (capacidad, consentimiento, nulidad). Además, excluye ciertas materias, como las ventas de títulos y valores mobiliarios, de navieros, barcos, electricidad y sobre todo, las ventas de las mercancías compradas para uso personal, esto es, la venta a consumidores.

Se aplica a las ventas realizadas por medios telemáticos. Nombra el teléfono, el telex y el fax, pero no menciona la Internet. A pesar de ello, se cree que ésta también

²¹⁹ Artículo 1 de la Convención de Naciones Unidas sobre la Compraventa Internacional de Mercaderías.

quedaría incluida en su ámbito de regulación, ya que este medio de compra ha alcanzado, e incluso desplazado, a aquéllos citados.²²⁰

Sin embargo, existen una serie de elementos que la hacen insuficiente para reglamentar los contratos a través del Internet:

1. La Convención de Viena implica la creación de un derecho uniforme de la compraventa, a pesar de que sólo ha sido ratificada por cerca de cincuenta países. Esto debiera ampliarse para regular el comercio mediante Internet.

2. Delimita las compraventas, excluyendo la venta a los consumidores.

3. Establece excepciones, tales como el objeto de la Convención, las reservas de los Estados, las reglas de orden público, la voluntad de las partes.

Entre las Convenciones de carácter general que permiten determinar la ley aplicable se encuentran:

- La *Convención de la Haya del 15 de Junio de 1955, sobre Ley aplicable a las compraventas con carácter internacional de bienes muebles corporales*.

Entró a regir el 1 de septiembre de 1964 y fue ratificada por muy pocos países. Entre ellos, Bélgica, Dinamarca, Finlandia, Francia, Italia, Nigeria, Noruega, Suecia y Suiza.

Prescribe la aplicación de la *ley del vendedor* como regla principal de Derecho Internacional Privado para la venta internacional, por lo que constituye el sistema de resolución de conflictos de normas que se aplica automáticamente en defecto de cláusula contractual.

La Convención se aplica a las compraventas de carácter internacional de *bienes corporales muebles*, por lo que no afecta a las prestaciones de servicios, ni la venta de objetos incorporeales.²²¹

- El *Convenio de Roma sobre la Ley aplicable a las obligaciones contractuales* del 19 de Junio de 1980.

Entró en vigor sólo después del 1 de Abril de 1991 y es hoy el Derecho Internacional Privado de los contratos de los estados de la Unión Europea que lo han ratificado.

²²⁰ Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, op. cit., pág.29.

²²¹ Candelario Macías, Isabel, "Breves apuntes sobre la normación del Comercio Electrónico", (c 2000, IBDI). Sitio Web Instituto Brasileiro de Política e Direito da Informática (IBDI) (<http://www.ibdi.hpg.ig.com.br/artigos/>), http://www.ibdi.hpg.ig.com.br/artigos/isabel_candelario/001.html , apartado 2.

El Convenio se aplica dentro del ámbito de las obligaciones contractuales. Es una norma de conflicto que puede *reenviar a la aplicación del Derecho interno* de uno de los estados involucrados.

Sin embargo, existen ciertas materias excluidas de su reglamentación, como los derechos y obligaciones de familia, las obligaciones nacidas en el ámbito cambiario, las obligaciones que surgen del derecho de sociedades y los contratos de seguros.

Este Convenio consagra un criterio universal, por lo que la ley designada por éste, se aplica incluso si tal ley es la de un estado no contratante.²²² También consagra la autonomía de la voluntad de las partes. Otorga libertad para que las partes elijan la ley aplicable a sus contratos.²²³

Ahora bien, si las partes no optan por determinada ley para regular sus actos, el Convenio establece que el contrato se regirá por la *ley del país “con el que presente vínculos más estrechos”*. Se presume que éste será el país en que la parte que deba realizar la prestación característica tenga su *residencia habitual*, o si se trata de una persona jurídica, *la administración central*, ello al momento de celebrarse el contrato.²²⁴

Se establecen otras disposiciones particulares respecto a los inmuebles, al contrato de transporte y al contrato individual de trabajo. También, para los contratos concluidos por los consumidores, los que no pueden ser privados de la protección que les otorgan las normas imperativas de la ley del país en el cual una de las partes tenga su residencia habitual.

8.4.2. La opinión de los Organismos Internacionales.

A nivel internacional, varias son las instituciones que pretenden obtener uniformidad de las reglas aplicables al comercio electrónico.

²²² Convenio sobre ley aplicable a las obligaciones contractuales, Roma 19 de Junio de 1980, artículo 2.

²²³ Convenio sobre ley aplicable a las obligaciones contractuales, Roma 19 de Junio de 1980, artículo 3.

²²⁴ Convenio sobre ley aplicable a las obligaciones contractuales, Roma 19 de Junio de 1980, artículo 4.

La *UNCITRAL*, en el año 1996, formuló la ya citada *Ley Modelo sobre Comercio Electrónico*.²²⁵ Ésta reúne diversos aspectos jurídicos del intercambio de datos informatizados y de medios de comunicación conexas.²²⁶

Su objetivo es constituir reglas comunes para eliminar los obstáculos y la incertidumbre que produce el uso de las modernas técnicas de comunicación en el Derecho Mercantil Internacional.

La *OCDE*²²⁷, en un informe publicado en 1997, postula una reforma de prácticas reglamentarias y una clarificación de las leyes aplicables a los siguientes ámbitos: protección del consumidor, confidencialidad, competencia, sistemas financieros y de pago, propiedad intelectual, tratamiento de conflictos y protección contra la criminalidad.²²⁸

La *Unión Europea* también es partidaria de un consenso a nivel internacional. Para ello ha dictado algunas directivas sobre aspectos ligados al comercio por la vía electrónica. Quizás la más importante es la *Directiva relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior o Directiva de Comercio Electrónico*, aprobada por el Parlamento Europeo el 4 de Mayo de 2000.

Esta directiva adopta el principio del “país de origen” el cual regirá la elección de la ley aplicable a los servicios *on line*.²²⁹ Así, esta norma dispone que los negocios de comercio electrónico establecidos en la Unión Europea sólo se encuentran sometidos a las leyes del país de su establecimiento.²³⁰ Agrega, además, que considera que el lugar de establecimiento de un negocio de *e-commerce* es aquel donde se encuentra efectivamente establecido por un tiempo indeterminado, sin que la ubicación física de

²²⁵ UNCITRAL (Comisión de Naciones Unidas para el Derecho Mercantil Internacional), *Ley Modelo sobre Comercio Electrónico*, aprobada en su vigésimo noveno período de sesiones, correspondiente al quincuagésimo primer período de sesiones de la Asamblea General de Naciones Unidas, 12 de Junio de 1996.

²²⁶ Candelario Macías, Isabel, “Breves apuntes sobre la normación del Comercio Electrónico”, op. cit., apartado 2.

²²⁷ Organización para la Cooperación y Desarrollo Económico.

²²⁸ Candelario Macías, Isabel, “Breves apuntes sobre la normación del Comercio Electrónico”, op. cit., apartado 2.

²²⁹ Vinje, Thomas C., “La Directiva de la Unión Europea en materia de Comercio Electrónico”, *Revista Derecho y Nuevas Tecnologías*, N° 3, Año 2, Editorial AD. HOC, Buenos Aires, Argentina, 2000, pág. 88.

²³⁰ Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de Junio de 2000, artículo 3.

los equipos, como los servidores, sean indicativos del establecimiento de una empresa en un determinado país.²³¹

²³¹ Vinje, Thomas C., “La Directiva de la Unión Europea en materia de Comercio Electrónico”, *Revista Derecho y Nuevas Tecnologías*, N° 3, Año 2, Editorial AD. HOC, Buenos Aires, Argentina, 2000, pág 89.

CAPÍTULO II.

EL DOCUMENTO ELECTRÓNICO.

1. Generalidades.

Como se indicó en el capítulo anterior, toda operación de comercio electrónico tiene como común denominador un contrato, a través del cual las partes materializan sus transacciones. Este contrato, da origen al *documento jurídico-electrónico*.

El documento electrónico debe ser analizado como segundo punto dentro del tema del comercio electrónico, ya que para su crecimiento y desarrollo, resultan fundamentales el reconocimiento legal, la equivalencia con el documento impreso en papel y la admisibilidad como medio de prueba.

Estos requisitos son imprescindibles para que el comercio realizado mediante la Internet sea atractivo tanto para consumidores como empresarios. Éstos requieren que los documentos que emanen de sus actuaciones en el ciberespacio, gocen de certeza jurídica, la que sólo se alcanza a través de una adecuada protección legal. Es la forma de lograr que estos sujetos confíen en que, ante cualquier divergencia, los tribunales estarán ahí para respaldarlos, al igual que en las operaciones comerciales tradicionales.

En el presente capítulo, se tratará, en una primera parte, *el documento en sentido genérico*, para recordar su concepto, clasificación y estructura.

Luego se analizará el *documento electrónico propiamente tal* con el propósito de determinar sus elementos y especiales características, lo que permitirá determinar su naturaleza jurídica. Parece interesante determinar si se constituye en una nueva clase de documento, con formalidades propias, o si por el contrario, se trata de un documento, al igual que el impreso clásicamente.

Especial atención merece su *reconocimiento como medio de prueba y su valor*, atendido el sistema probatorio imperante en Chile. De ello dependerá la fuerza que el juez le otorgue para acreditar, en el caso específico del contrato, su existencia y obligatoriedad, así como para exigir el cumplimiento forzado de la obligación que surge

de él, lo que como ya se indicó, se convierte en una suerte de garantía para los comerciantes. En este punto cobra importancia la *Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*.²³²

2. El documento en sentido genérico.

2.1. Concepto.

La mayor parte de los ordenamientos jurídicos en el mundo utilizan el vocablo documento, sin señalar un concepto del mismo. Es labor de la doctrina y de la jurisprudencia establecer su contenido y alcance, traduciéndose ello en una gran cantidad de definiciones y puntos de vista.

Para el *Diccionario de la Lengua Española* “documento”, en sentido amplio, es “cualquier (...) cosa que sirve para ilustrar o comprobar algo”²³³, por lo que puede tratarse de documentos jurídicos, comerciales, económicos, históricos o, en general, cualquier manifestación del pensamiento del hombre.

En un sentido parecido se pronuncia Carnelutti, que lo concibe como “una cosa u objeto que mediante la intervención de la actividad del hombre, es capaz de representar un hecho.”²³⁴

La legislación chilena, al igual que muchas en el derecho comparado, guarda silencio a la hora de indicar un concepto, por lo que a la luz del artículo 20 del Código Civil, la palabra documento debe ser entendida en su sentido natural y obvio.²³⁵ De la misma forma, la jurisprudencia se refiere a éste sin definirlo.

En doctrina, los autores se aventuran en *concepciones amplias y restringidas*. Así por ejemplo, algunos, tienden a identificarlo con “aquellos escritos en soporte de papel

²³² Publicada en el Diario Oficial el 12 de abril del año 2002.

²³³ Real Academia Española, *Diccionario de la Lengua Española*, op. cit., pág. 491.

²³⁴ Carnelutti, Francesco, *Sistema de Derecho Procesal Civil*, Volumen II, UTEHA (Unión Tipográfica Editorial Hispano Americana), Buenos Aires, 1944, (tr. Niceto Alcalá-Zamora y Castillo y Santiago Sentís Melendo), pág. 414, citado por Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 80.

²³⁵ El artículo 20 del Código Civil establece que “Las palabras de la ley se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras (...)”.

y rubricados manualmente.”^{236 237} Otros, admiten en forma genérica, que es “*cualquier objeto que contiene una información, que narra, hace conocer o representa un hecho, cualquiera sea su naturaleza, su soporte o “continente”, su proceso de elaboración o su tipo de firma.*”^{238 239}

En esta última concepción, la característica de *escrito* no se presenta como algo esencial del documento, lo que permitiría, en una primera aproximación, incluir al documento electrónico dentro del concepto general de documento.

2.2. Documento e instrumento.

Las legislaciones mundiales herederas del Código Napoleónico, incluidas entre ellas la chilena, tienden a utilizar como sinónimos los vocablos *documento e instrumento*.

Sin embargo, a pesar de su carácter legal, tal identificación no parece correcta, toda vez que *instrumento* es “un escrito firmado en que se exterioriza o manifiesta el pensamiento del autor”.²⁴⁰

Documento, en cambio, tiene un carácter genérico y se emplea para referirse a cualquier “medio externo demostrativo de una idea”.²⁴¹ Así concebido, el documento es un concepto más amplio, que comprende todo objeto demostrativo de una idea o pensamiento, como los dibujos, los cuadros, las fotografías, las películas, etc.

²³⁶ Para el profesor chileno Mario Casarino, por ejemplo, el documento es “todo escrito en que se consigna un hecho”. Casarino Viterbo, Mario, *Manual de derecho procesal. Derecho procesal civil*, Tomo IV, Quinta Edición, Editorial Jurídica de Chile, Santiago, Chile, 2000, pág. 97.

²³⁷ Jijena Leiva, Renato Javier, “Naturaleza jurídica y valor probatorio del documento electrónico. El caso de la declaración de importación electrónica o mensaje CUSDEC”, *Revista de Derecho de la Universidad Católica de Valparaíso*, N° XIX, Ediciones Universitarias de Valparaíso, Valparaíso, Chile, 1998, pág. 458.

²³⁸ Ibid.

²³⁹ Alfredo Etcheberry también señala de manera amplia que documento es “*todo objeto que representa un hecho o una manifestación de pensamiento, emanado de un autor y fijado en forma permanente*”. Etcheberry, Alfredo, *Derecho Penal*, Tomo IV, Parte Especial, Tercera Edición (revisada y actualizada), Editorial Jurídica de Chile, Santiago, Chile, pág. 156 y 157.

²⁴⁰ González, Adriana; Marino, Adela y Carrica, Pablo, “Instrumentos públicos, privados y particulares”, *Revista Notarial*, N° 897, Argentina, 1988, pág. 444; citado por Ruiz, Fernando, “El documento electrónico frente al derecho civil y financiero”, *Revista de Derecho Informático (REDI)*, N° 16, Noviembre 1999 (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/>; Histórico), <http://www.alfa-redi.org/revista/revista.asp?idRevista=16#>, pág. 23.

²⁴¹ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 97.

El instrumento, se constituye en una categoría especial de documento, formada por aquellos *escritos* destinados a consignar una *relación jurídica*. En consecuencia, es de su esencia el ser escrito y de carácter jurídico.²⁴²

A pesar de sus diferencias, el legislador utiliza ambas palabras indistintamente, como sinónimas. Por ello sólo su determinación de *público o privado* les dará el valor que el derecho requiere para calificarlos.²⁴³

Tres son los elementos que permiten calificar al instrumento de público o privado: el pensamiento, el contenido y el autor.

El *pensamiento*, implica el querer del autor respecto a lo que ha pretendido plasmar en el documento. Éste no expresa el hecho ocurrido en el mundo externo sino que la manifestación intelectual de su autor. El *autor* es quien interviene en su realización, el que debe ser reconocido por el destinatario.²⁴⁴ Por último, el *contenido*, se refiere al hecho jurídico relatado en él, el que puede ser manifestado mediante formas, las que consisten en un marco a través del cual el hecho se hace perceptible en el ámbito jurídico.²⁴⁵

2.3. Clasificación.

Los instrumentos admiten diversas clasificaciones atendiendo distintos puntos de vista. En esta oportunidad, se recordará aquella que atiende a su origen, y que los divide en públicos y privados.

El *instrumento público o auténtico*, definido por el artículo 1699 del Código Civil, “es el autorizado con las solemnidades legales por el competente funcionario”.

Los *instrumentos privados*, no son conceptualizados por el legislador nacional, por lo que por exclusión, se definen como “aquellos que dejan constancia de un hecho sin

²⁴² Alsina, Hugo, *Tratado Teórico Práctico de Derecho Procesal Civil y Comercial*, T. III, pág. 391. Cit. por Dunlop, Nelly. *El Reconocimiento del Instrumento Privado*, pág. 9. Memoria, U. de Chile, Editorial Universitaria, Santiago, 1965; citado por Ruiz, Fernando, “El documento electrónico frente al derecho civil y financiero”, op. cit., pág. 23.

²⁴³ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 83.

²⁴⁴ Ello dependerá de la teoría acogida. Según la *teoría de la firma*, es autor del documento, quien lo firma. En virtud de la *teoría de la compilación*, es autor quien le da forma intelectualmente al instrumento. La *teoría del autor del pensamiento*, señala que es autor del documento, quien efectúa la declaración que se hace mediante el documento.

²⁴⁵ Dependerá de la clase de documento: *ad substantiam*, *ad solemnitatem* o *ad probationem*. Los primeros requieren de formas sustantivas para su perfección. Los segundos, de solemnidades en consideración al acto y no al documento. Y los *ad probationem*, se refieren no a la forma del documento sino a su prueba.

solemnidad alguna (...), en cuyo otorgamiento no interviene un funcionario en calidad de tal (...). Además, “no llevan en sí ningún sello de autenticidad”.²⁴⁶

La principal importancia de esta diferenciación radica en que los instrumentos públicos, por el cumplimiento de las formalidades requeridas y por la intervención del funcionario competente, poseen características de seguridad, autenticidad, integridad y permanencia, de las que carece el instrumento privado.²⁴⁷

Es por esto que el legislador les otorga el máximo valor probatorio, como lo señala el artículo 1700 del Código Civil: “El instrumento público hace plena fe en cuanto al hecho de haberse otorgado y su fecha, pero no en cuanto a la verdad de las declaraciones (...)”.

No ocurre lo mismo con los instrumentos privados. Sin embargo, la legislación procesal acepta la posibilidad de tenerlos legalmente por reconocidos, con lo que se les daría cierta autenticidad.²⁴⁸

2.4. Estructura del documento.

Como ya se indicó, el documento es una cosa que representa algo. Aquella cosa se compone de dos elementos. Uno corporal o material, y el otro intelectual.

2.4.1. Elemento material.

Es el *cuerpo o soporte del documento*, formado por el *corpus* y la *grafía*.

Al hablar de *corpus* o *cosa corporal*, se refiere al papel, pero también al actualmente adoptado soporte electrónico. Es decir, se habla de la cosa o elemento material que conforma el documento.²⁴⁹

La *grafía*, constituida normalmente por la escritura, es el medio de expresión incorporado por el autor al cuerpo del documento.

²⁴⁶ Jijena Leiva, Renato Javier, “Naturaleza jurídica y valor probatorio del documento electrónico. El caso de la declaración de importación electrónica o mensaje CUSDEC”, op. cit., pág. 459.

²⁴⁷ Ibid.

²⁴⁸ En el artículo 346 del Código de Procedimiento Civil se indican las cuatro formas de tener por reconocido un instrumento privado.

²⁴⁹ En tiempos pasados era común encontrar pergaminos, papiros, trozos de metal, etc.

Contiene dos aspectos: uno *físico o estático*, relativo a los diversos instrumentos utilizados para escribir,²⁵⁰ y otro *dinámico o esencial* que se constituye en un enlace entre la mente del autor y la corporeidad del instrumento.

El aspecto dinámico es propiamente la opinión del autor, vale decir, el proceso volitivo e intelectual deseado por éste, la causa o razón de la confección documental. Es por esto que no hay documento casual. Éste siempre resulta de un deseo de su autor, sin el cual el documento no nace. Por ello, los autógrafos no son documentos en sentido jurídico.²⁵¹

2.4.2. Elemento intelectual, ideológico o docente.²⁵²

Dos son los aspectos ideológicos del documento:

a) La conciencia o intención de expresión. El autor debe, al momento de la formación del documento, *desear expresar* un contenido a través de él.

b) La expresividad explicativa del autor. El creador, objetivamente, debe *reconocer* lo expresado en el documento. Se trata de una relación entre el autor y el destinatario, que debe emanar claramente y a consecuencia de lo expresado en el instrumento.

La expresividad deberá ser: *objetiva, transitiva en su contenido y reconocible*.

Mediante la *objetividad* el autor expone su pensamiento al mundo exterior, haciéndolo patente y estabilizándolo en el documento. Por esto, una minuta de escritura pública no puede ser considerada documento, ya que no expresa el pensamiento del autor.

Ahora bien, la *reconoscibilidad* permite que el mensaje dirigido por el autor sea recibido por el destinatario. A través de ella, es posible establecer *su autor, su contenido y los medios de expresión* a que se ha recurrido.²⁵³

El documento debe permitir que el *autor* sea identificado o reconocido. Es por esto que los anónimos no son documentos.

²⁵⁰ Respecto a los medios para plasmar sobre el *corpus*, Eugenio Gaete distingue entre: *calamus* (tinta, cinta de la máquina de escribir, entre otros), e *incaustus* (la pluma de ave en un comienzo, la pluma de metal, los modernos métodos de impresión, como los computadores, impresoras láser, etc.). Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 169.

²⁵¹ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 113.

²⁵² Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 114.

²⁵³ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 85.

En cuanto al *contenido*, éste debe ser *transitivo*, es decir, dotado de significación jurídica. Además, debe ser comunicado a otras personas, por lo que no debe ser secreto.

Por último, la grafía debe ser fijada de alguna manera. Esto se logra mediante los elementos formales o *medios de fijación*, como son:

- Las formas escritas clásicas y nuevas, como el manuscrito, el grabado, la impresión, el fotograbado, el mecanografiado, el efectuado en sistema *offset*,²⁵⁴
- La fotografía y sus derivaciones;
- El sistema documental electrónico, a través del cual nace un nuevo medio de fijación, ya que deja constancia gráfica mediante el uso del computador y de ciertos sistemas de claves que garantizan su existencia y permanencia.²⁵⁵

3. El documento emitido por medios electrónicos.

3.1. Concepto.

El documento electrónico no responde al concepto restringido de documento, impreso en papel, sino a aquel descrito como amplio.²⁵⁶

Entonces, como primera aproximación, y por descarte, se puede decir que constituye un documento no electrónico aquel que es elaborado por los mecanismos clásicos, sean manuales, mecanográficos o fotográficos.

Ahora bien, según la forma en que el documento electrónico ha sido elaborado, es posible abordarlo desde dos puntos de vista:

a) En un *sentido estricto*, el *instrumento electrónico* se refiere a los “casos en que el *lenguaje magnético* constituye la acreditación, materialización o documentación de una voluntad, probablemente ya expresada en las formas tradicionales, y en que la actividad de un computador o de una red sólo comprueban o consignan electrónica, digital o

²⁵⁴ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit. pág. 115.

²⁵⁵ Ibid.

²⁵⁶ Es decir “cualquier objeto que contiene una información, que narra, hace conocer o representa un hecho, cualquiera sea su naturaleza, su soporte o “continente”, su proceso de elaboración o su tipo de firma.” Cfr. Capítulo II, apartado 2.1.

magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes.”²⁵⁷

Esta clase de documentos sólo pueden ser percibidos y entendidos por el ser humano una vez traducidos a un lenguaje natural, debido a que están elaborados en forma digital, mediante un sistema alfanumérico o similar. Ejemplo de éstos son los documentos expresamente creados para el uso de las terminales de un sistema, como las tarjetas magnéticas.²⁵⁸

b) *El documento electrónico en sentido amplio*, incluye tanto a aquellos documentos que constan de manera digital como a los elaborados en un lenguaje natural. Éstos últimos, pueden ser apreciados directamente por el hombre, sin la intervención de una máquina traductora. Pueden ser leídos desde la pantalla, o utilizando una impresora, desde un soporte papel. Ejemplo de éstos sería el comprobante que emite un cajero automático o un correo electrónico impreso.²⁵⁹

3.2. Concepto legal de Documento Electrónico.

La mayor parte de las legislaciones mundiales han optado por dictar leyes que permitan la aplicación del documento electrónico, evitando por esta vía, las dudas que pudiera generar su incorporación al mundo del derecho a través de la interpretación legal.

Chile, por medio de la ya citada *Ley 19.799 sobre Documentos electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma*, adopta un estatuto particular sobre el tema.

En su artículo 2º define, entre otras cosas, al *documento electrónico* como “toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o

²⁵⁷ Jijena Leiva, Renato Javier, “Naturaleza jurídica y valor probatorio del documento electrónico. El caso de la declaración de importación electrónica o mensaje CUSDEC”, op. cit., pág. 460.

²⁵⁸ Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 59.

²⁵⁹ Herrera Bravo, Rodolfo, “El documento electrónico: algunas vías de aplicación en el Derecho Probatorio Chileno”, *Revista de Derecho Informático (REDI)*, N° 7, Febrero 1999, (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/8-4.asp> , apartado 1., Introducción.

recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior”.²⁶⁰

3.3. Clasificaciones.

1) Según el papel que le cabe al computador en la creación del documento electrónico, se distingue entre:

a) Documento formado por el computador.

En este primer caso, el computador, de acuerdo a una serie de parámetros y datos, y conforme a un programa determinado, *decide* en el caso concreto, el contenido de una regulación de intereses. Este es el caso del acto jurídico concluido por medio del computador o entre ordenadores.^{261 262}

En esta situación, el computador no se limita a documentar la voluntad, sino que determina su contenido. Sin embargo, no se debe olvidar que se habla de un artefacto, sin voluntad propia, por lo que requiere de instrucciones emanadas del hombre de manera más o menos concreta.²⁶³

Este sistema cada vez adquiere más importancia, especialmente en la contratación a gran escala.²⁶⁴

b) Documento formado por medio del computador.

En esta categoría, el computador *documenta* una regulación de intereses ya expresados en otras formas. Su función está destinada sólo a documentar y no a constituir.

Se trata de la situación más común, donde se puede distinguir entre:

²⁶⁰ Ley 19.799, artículo 2º, letra d.

²⁶¹ Cfr. Capítulo I, apartado 4.1.1.

²⁶² Ruiz, Fernando, “El documento electrónico frente al derecho civil y financiero”, op. cit., pág. 33.

²⁶³ Carrascosa López, Valentín, et al., *La Contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 58.

²⁶⁴ Recuérdese lo señalado a propósito de EDI en la parte introductoria de este trabajo, apartado 4.2.8.3.

b.1.) Documento electrónico en sentido estricto.²⁶⁵

Es aquel que no puede ser leído directamente por el hombre sin la intervención de una máquina que haga perceptible y comprensible la señal digital que lo constituye.

Puede estar contenido en la memoria central del computador o en otra clase de soporte, como el CD-ROM, diskette, zip disk, etc.

Atendido el “grado de perdurabilidad en el tiempo” (lo que dependerá del modo de elaboración y del soporte), esta clase de documentos electrónicos pueden, a su vez, ser:²⁶⁶

b.1.1.) Volátiles. Son aquellos que se pierden una vez que el computador deja de funcionar, como ocurre por ejemplo con los datos contenidos en las memorias circuitales RAM (*Random Access Memory*).

Esta clase de documentos no estarían incluidos en el concepto del artículo 2 de la Ley 19.799, ya que ella exige que sea “almacenada de un modo idóneo para permitir su uso posterior”.

b.1.2.) Permanentes. Corresponde a aquellos cuya información sólo desaparece al ser eliminada o borrada. En caso contrario, se mantiene en el tiempo. Generalmente están contenidos en discos magnéticos, como los floppy disks (conocidos más comúnmente como diskettes), zip disks, o hard disks (discos duros); también en discos ópticos borrables o EO disks (*erasable optical*).

b.1.3.) Inalterables. Se refiere a los documentos que no pueden ser modificados, sino sólo leídos. Para ello se utilizan, por ejemplo, las memorias ROM (*Read Only Memory*), que consisten en un circuito integrado al computador o incorporado a voluntad, y los CD-ROM, que son una memoria de masa contenida en un disco láser.

b.1.4.) Access Devices (medios de acceso). Se trata de los documentos creados para el uso de los terminales de un sistema. Ejemplo de ellos son las tarjetas magnéticas.²⁶⁷

²⁶⁵ Algunos autores lo denominan documento informático. Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 169.

²⁶⁶ Altmark, Daniel Ricardo, “Valor Jurídico del Documento Electrónico en el Derecho Argentino”, Ponencia presentada en el IV Congreso Iberoamericano de Informática y Derecho, Bariloche, 1994, citado por Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 58.

²⁶⁷ El nombre corresponde al dado por el *New Payment Code*, de Estados Unidos, en los artículos 50 y 201: “A card, check, code passbook or any other means of access to an account, or any necessary combination thereof, that may be used to initiate an order”.

b.2.) Documento electrónico en sentido amplio o de origen electrónico.

Se refiere a la serie de documentos que pueden tener su origen en el computador mediante sus órganos de salida. Éstos no estarán escritos en lenguaje digital, sino en un texto alfanumérico, en un gráfico impreso en papel, en una tarjeta o cinta perforada, y en general, en cualquier objeto material con las características de un documento formado por una máquina conectada con un ordenador.²⁶⁸

Estos documentos son legibles por el hombre de manera directa, mediante el monitor o una impresora, sin la utilización de equipos traductores. En realidad se trata de copias del documento electrónico en sentido estricto.

2) Según su modo de formación, los documentos electrónicos se dividen en:

a) Por intervención humana.

El documento es guardado en la memoria del computador, de manera directa por el hombre (tecleándolo por ejemplo).

b) Por intervención de una máquina.

Se trata de los casos en que el documento es introducido en la memoria a través de un artefacto, como un lector óptico o scanner.

La importancia de esta clasificación radica en que la incorporación a la memoria de un documento preexistente contenido en papel, puede efectuarse mediante la *transcripción* del documento en un lenguaje electrónico o por la *reproducción* completa y fiel de la forma y del contenido del documento original.

En la primera situación, nace un documento nuevo, aún si su contenido es idéntico al del documento transcrito. En la segunda, no se trata de transcribir un documento, sino de la reproducción automática de su forma y contenido. En efecto, no se trata sólo de registrar sobre un soporte los caracteres alfabéticos o numéricos contenidos en el documento, sino que de efectuar una función más compleja que incluye la reproducción de la imagen del documento, la división de dicha imagen en una serie de elementos uniformemente distribuidos, denominados PEL (*picture elements*), y la transformación

²⁶⁸ Ruiz, Fernando, “El documento electrónico frente al derecho civil y financiero”, op. cit., pág. 34.

de tales puntos a lenguaje digital, de manera que puedan ser conservados en la memoria. El resultado, no es la simple transcripción sino la reproducción completa y exacta de la forma y del contenido documental preexistente.²⁶⁹

3.4. Composición del documento electrónico atendidos los requisitos del documento tradicional.

Si se parte de la base que el documento informático tiene un carácter documental, se puede concluir que debe reunir los requisitos establecidos para el documento en general, indicados al comienzo de este capítulo.²⁷⁰

Sin embargo, como se verá a continuación, ellos adquieren ciertos matices.

3.4.1. Elemento material del documento electrónico.

El *corpus* en el documento electrónico, se ve modificado en relación al instrumento *per cartam* o tradicional. Esto no significa que se le reste su calidad documental, ya que desde un ámbito funcional, sigue siendo *una cosa que sirve para representar un hecho*.²⁷¹

En este caso, la corporalidad del documento estará constituida por el soporte electrónico, que puede adoptar diversas formas. Puede ser magnético, como los diskettes, los zip disks, o los discos duros del computador, u óptico, como los CD-ROMs, EO disks o WORM disks.²⁷²

La *grafía o medio de expresión*, no será la tradicional escritura, ya que ésta es reemplazada por un lenguaje no natural, que para ser legible y entendible por el hombre, requiere de traducción. Se trata del método utilizado por las computadoras en la fase de

²⁶⁹ Ruiz, Fernando, “El documento electrónico frente al derecho civil y financiero”, op. cit., pág. 35.

²⁷⁰ Cfr. Capítulo II, apartado 2.4.

²⁷¹ Es un medio de representación (al decir de Carnelutti), y como tal pueden existir distintas clases de representaciones reales: la escritura en soporte papel, las fotografías, el cine, y por qué no agregar, los derivados de la electrónica, como el correo electrónico, el fax, la contratación vía EDI, etc. Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 255.

²⁷² Los *EO disks* (erasable optical) son un tipo de disco óptico que puede ser borrado. El *WORM disk*, abreviatura de “write-once, read-many”, es otra clase de disco óptico que puede ser escrito una sola vez, pero leído muchas veces. Sin embargo, a diferencia del CD-ROM, sólo puede ser leído por el mismo *disk drive* utilizado para escribirlo, lo que lo hace menos popular (El *disk drive* es el equipo que escribe y lee disks o discos).

elaboración del mensaje: un sistema de comunicación digital de símbolos, denominado *Código Binario*.²⁷³

3.4.2. Elemento intelectual del documento electrónico.

Respecto al *pensamiento*, ni la *expresividad objetiva* ni la *reconosibilidad* se ven modificadas en el documento electrónico.

En cuanto al *contenido*, el principal inconveniente surge en relación a la suscripción del mismo. El documento electrónico, generalmente, es un instrumento celebrado a distancia por lo que carecerá del requisito de la firma, entendida ésta en su concepto tradicional. Ella es reemplazada satisfactoriamente por la *firma digital*,²⁷⁴ la que constituye un sistema eficaz para asegurar el contenido del documento, así como “la aquiescencia prestada a éste por la parte correspondiente”,²⁷⁵ cumpliéndose perfectamente el requisito de la suscripción.

El problema de la *autoría del documento* se soluciona mediante la individualización obligatoria de las partes y de la autoridad certificadora, que otorga el certificado necesario para encriptar la firma digital del interesado originador o destinatario del mensaje de datos.

A modo de conclusión se puede indicar que la verdadera diferencia entre el documento tradicional y el electrónico está en su componente material.

3.5. Naturaleza jurídica del documento electrónico.

Como se ha señalado, las variaciones en el documento electrónico se refieren a cambios en aspectos materiales del mismo. Se modifica su corporalidad, de tal forma que su soporte será un sistema de conformación electrónica, expresado mediante un lenguaje binario. A pesar de ello, responde a la concepción amplia de documento (una cosa que representa un hecho).

²⁷³ Cfr. Capítulo II, apartado 3.6.

²⁷⁴ Según el artículo 2 de la Ley 19.799, la firma electrónica es “cualquier sonido, símbolo o proceso electrónico, que permite el receptor de un documento electrónico identificar al menos formalmente a su autor”.

²⁷⁵ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 194.

Por esto, las discusiones no se dirigen en determinar si es o no un documento, ya que al parecer, nadie le niega tal carácter. Las dudas se relacionan con su calidad documental.

Se pueden resumir en dos las corrientes que surgen al respecto.

Por un lado, se señala que el documento electrónico corresponde a una *nueva forma de documento*, el cual requiere del establecimiento de nuevas formalidades.

Esto debido a las diferentes mutaciones generadas en la concepción documental clásica. Así, por ejemplo, la modificación del lenguaje de comunicación. Como se ha mencionado, este nuevo instrumento utiliza un sistema o código binario, y no el lenguaje común al que se está acostumbrado.

Otros, creen que es el *mismo documento tradicional o per cartam*, al cual se le han agregado nuevas variantes, las que no le restan sus cualidades esenciales ni su objeto.

Los defensores de esta postura se basan en la concepción amplia de documento, particularmente en Carnelutti, por lo que mediante la interpretación, pretenden adaptar la legislación clásica al documento electrónico.

En Chile, el documento electrónico encuentra reconocimiento legal mediante la *Ley 19.799*, la que lo trata en forma especial, sin incorporarlo a la legislación documental tradicional. Esto, unido a sus especiales características y a las modificaciones al documento per cartam, especialmente la relativa al lenguaje, se traduce en que, al parecer, se trata de una *nueva forma de documento*.

3.6. El lenguaje del documento electrónico.

Como se ha adelantado, el documento informático o electrónico en sentido estricto utiliza un lenguaje especial, denominado *sistema binario*.

Éste difiere del *lenguaje natural*²⁷⁶ empleado por el hombre y los documentos electrónicos en sentido amplio, porque no puede ser leído directamente, sin la intervención de programas traductores.

El documento informático está dirigido a un medio constituido por computadores y no por personas, por lo que la falta de entendimiento directo no reviste inconveniente alguno en su consideración documental.

²⁷⁶ El lenguaje natural es el utilizado por los seres humanos para comunicarse, como el inglés, el español, el francés, etc.

3.6.1. Código Binario.

El *Código Binario* es un lenguaje simbólico para representar información, denominado así, porque utiliza dos valores únicos: 0 y 1. Ellos, debidamente combinados, representan diversas clases de datos.

Está compuesto por sólo dos dígitos, debido a que el computador, formado por circuitos eléctricos, utiliza el voltaje para lograr cierto discernimiento: 5 volts y 0 volts, (o lo que es lo mismo, conducción o no conducción), representados por 1 y 0 respectivamente.

Cada número, 1 ó 0, es un *bit (binary digit)* correspondiendo a la unidad más pequeña de información en un computador. Datos más complejos se obtienen combinando, consecutivamente, bits en unidades más grandes. Por ejemplo en *byte*, compuesto por ocho bits consecutivos.

En definitiva, para que el computador comprenda las instrucciones que se le han impartido en lenguaje natural, sean letras, números, signos de puntuación, etc. es necesario que éstas se encuentren representadas en lenguaje binario.

3.6.2. Lenguajes de interpretación.

Ha quedado claro que las comunicaciones de datos dentro del computador y entre computadores se realizan en código binario.

Sin embargo, como éste resulta ininteligible para el hombre, se recurre a programas que utilizan un *lenguaje de interpretación*.

Estos programas, llamados técnicamente, *aplicaciones*, utilizan un mecanismo que traduce a lenguaje binario, o viceversa, números decimales, letras, signos de puntuación, etc. escritos en lenguaje natural.

Así por ejemplo, en el estándar ASCII (*American Standard Code for Information Interchange*), que utiliza números del 0 al 127 para representar diversos caracteres del idioma inglés, la letra A (del lenguaje natural) es 065; B es 066, 0 es 048; 1 es 049, etc.

Una vez traducidos a ASCII, esto es a números decimales, la traducción a lenguaje binario es directa: El número 1 (en lenguaje natural) es 049 en ASCII y 00110001 en binario.

Además de ASCII existen otros lenguajes de interpretación, como ANSI (*American National Standards Institute*), o el universal, ISO Latin-1.

3.6.3. Etapas en la comunicación hombre-computador.

En la *fase de memorización*, la información que se recibe es ingresada en el computador. Ésta puede ser introducida por medio de cualquier *canal de transmisión*: teclado, mouse, scanner, etc.²⁷⁷

En la *fase de elaboración*, los datos son codificados o traducidos a lenguaje digital. Para ello, se requiere de programas o aplicaciones que emplean estándares internacionales (ASCII, ANSI, ISO Latin-1, etc.) para traducir la información a código binario.

Traducida la información a sistema binario, el computador puede comprender y efectuar todo tipo de operaciones.

Sin embargo, para que el hombre, pueda nuevamente comprender los resultados de dichas operaciones, se hace necesario volver la información a lenguaje natural. Para ello se realiza el proceso inverso: de binario, a través de un programa, se traduce a algún lenguaje de interpretación, y de éste, a lenguaje natural.

3.7. El documento electrónico de la Administración Pública.

Los documentos electrónicos no sólo adquieren relevancia en el ámbito privado. De los órganos del Estado también pueden emanar documentos de estas características.

Para ello es necesario el reconocimiento legal de esta posibilidad, así como también el fortalecimiento de la seguridad desde un punto de vista técnico y jurídico. Este es el objetivo que cumplió, en un principio, el *Decreto Supremo N° 81 del Ministerio*

²⁷⁷ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 205.

Secretaría General de la Presidencia²⁷⁸, de 1999, y que hoy cumple el *Título II de la Ley 19.799* y su *Reglamento*.

3.7.1. La Ley 19.799 en relación con el documento electrónico de los Órganos del Estado.²⁷⁹

La Ley autoriza a los órganos del Estado para que, *por medio de firma electrónica*, ejecuten o realicen actos, celebren contratos y expidan cualquier documento, dentro de su ámbito de competencia.²⁸⁰ Dichos actos, contratos y documentos adquieren plena validez, y producen idénticos efectos al impreso en soporte papel.

Sin embargo, para que tengan la calidad de *instrumento público*, la ley obliga a suscribirlos por medio de *firma electrónica avanzada*.

La certificación de las firmas electrónicas avanzadas de los funcionarios, debe efectuarse por los correspondientes ministros de fe, o en su defecto, por un funcionario designado para ello. Sin perjuicio de lo anterior, el estado puede contratar los servicios de un certificador acreditado.²⁸¹

A diferencia del Decreto Supremo N° 81, la Ley 19.799 y su Reglamento no sólo establecen normas para las comunicaciones electrónicas al interior de la Administración sino también para su relación con los particulares, los que deberán consentir expresamente en dicha forma de comunicación.²⁸²

Los documentos en que se relacionan personas y el Estado podrán estar firmados electrónicamente. Sólo se exige firma avanzada cuando se haga necesario comprobar fehacientemente la identidad.²⁸³

El Reglamento de la Ley 19.799 exige a los órganos del Estado llevar un *Repositorio* o archivo de documentos electrónicos con el fin de garantizar la seguridad, integridad y disponibilidad de tales documentos.

²⁷⁸ El Decreto Supremo N° 81 del Ministerio Secretaría General de la Presidencia fue derogado por el Artículo Segundo del Decreto Supremo N° 181 del Ministerio de Economía, Fomento y Reconstrucción.

²⁷⁹ Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, aprobado por el Decreto Supremo N° 181 del Ministerio de Economía, Fomento y Reconstrucción de 9 de Julio de 2002, publicado en el Diario Oficial el 17 de Agosto de 2002.

²⁸⁰ Sólo excluye a aquéllos cuyas solemnidades no puedan cumplirse electrónicamente. Artículo 6 de la Ley 19.799 y 39 del Reglamento.

²⁸¹ Artículo 9 de la Ley 19.799, 40 y 41 del Reglamento de dicha Ley.

²⁸² Artículo 8 de la Ley 19.799 y 53 del Reglamento.

²⁸³ Artículo 52 del Reglamento de la Ley 19.799.

También crea el *Comité de Normas para el Documento Electrónico*, organismo asesor encargado de la fijación de normas técnicas que permitan la comunicación entre los órganos estatales, y entre éstos y los particulares.

3.7.2. Leyes especiales.

Como parte del proceso de modernización del Estado de Chile se han introducido modificaciones a varias disposiciones especiales, las que permiten la utilización del documento electrónico en la actividad estatal, y entre ésta y los privados.

Así, por ejemplo, se puede mencionar las reformas a la *legislación tributaria* que permite la declaración de diversos impuestos por Internet.²⁸⁴ Se trata, entre otros, del artículo 30 del Código Tributario, el que ha dado lugar a varias resoluciones y circulares.²⁸⁵

En materia de Aduanas, la *Ordenanza General* en su artículo 71 constituye otro importante ejemplo.^{286 287}

4. Documentos privados y públicos electrónicos.

4.1. Requisitos propios del documento electrónico.

Para que el documento electrónico tenga valor jurídico debe, necesariamente, reunir las exigencias legales de todo documento tradicional o impreso en papel.

Así, según el profesor Eugenio Gaete,²⁸⁸ debe cumplir con los *requisitos instrumentales probatorios, propios de cualquier acto o contrato*, como ser instrumento público o privado de aquellos reconocidos por el Código Civil, y reunir las exigencias de eficacia que establecen las leyes de procedimiento para que tengan valor probatorio. También debe reunir los *requisitos de fondo exigidos por la ley del contrato*, respecto

²⁸⁴ Cerca de un millón de contribuyentes efectúa declaraciones mensuales del Impuesto al Valor Agregado y alrededor de dos millones declara y paga el Impuesto a la Renta.

²⁸⁵ Cfr. Capítulo II, apartado 5.2.2. letra c.

²⁸⁶ En Chile, anualmente, alrededor de 1,3 millones de personas realiza trámites aduaneros a través de documentos electrónicos.

²⁸⁷ Cfr. Capítulo II, apartado 5.2.2. letra g.

²⁸⁸ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 189.

del acto que se instituye en tal documento, atendiendo a su especie y a la calidad o al estado de las personas que lo ejecuta o acuerdan, bajo pena de nulidad del acto o contrato. Además, tiene que cumplir con las exigencias formales establecidas por la ley para el valor de ciertos actos, en consideración a la naturaleza de ellos, causa, consentimiento y objeto lícitos.²⁸⁹

Junto a éstos, debe reunir los *requisitos formales procesales*, es decir aquéllos establecidos para la validez del acto formal, como son: “lenguaje y estilo, enmienda y corrección de errores, rogación, los requisitos de la escritura pública, los deberes notariales -como lo son la autoría y responsabilidad, el control de legalidad, el deber de imparcialidad, el principio de inmediación y el deber de conservación- el otorgamiento de la escritura -lectura, consentimiento, firma, comparecencia de testigos- la autorización de la misma y los sistemas de archivo y reproducción de los instrumentos públicos”.^{290 291}

Con todas estas exigencias debe cumplir el documento electrónico para ser considerado un *instrumento público*. Sin embargo, en caso de incompetencia o falta de alguna solemnidad, valen como instrumentos privados, siempre que se encuentren firmados por las partes, en virtud del artículo 1701 inciso 2° del Código Civil.

En consecuencia, residualmente, todos aquellos documentos que no son instrumentos públicos, por faltarles algún requisito legal para ser considerados como tales, constituyen *instrumentos privados*.

4.2. El documento electrónico como instrumento público.

Según el artículo 1699 del Código Civil chileno el instrumento público o auténtico es “el autorizado con las solemnidades legales por el competente funcionario”. El inciso segundo agrega que “otorgado ante escribano e incorporado en un protocolo o registro público, se llama escritura pública.”

²⁸⁹ Se trata de cumplir con los artículos 1681 y 1682 del Código Civil, sobre la nulidad de los actos jurídicos.

²⁹⁰ Se refieren a la *matricidad*, es decir, al registro del documento original en el protocolo del notario, al otorgamiento de copias y al archivo del documento.

²⁹¹ Gaete González, Eugenio Alberto, “Documento electrónico e instrumento público”, *Revista de Derecho Informático (REDI)*, N° 24, Julio 2000, (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/25-8.asp> , apartado III.

En consecuencia, como primera aproximación, se puede afirmar que no existe inconveniente para calificar de público un documento electrónico, siempre que esté autorizado por un empleado público competente con las formalidades establecidas por la ley.

La intervención de un *funcionario competente* es perfectamente posible de realizar por medios electrónicos.²⁹² Sin embargo, la obligación de cumplir con las *solemnidades legales* sólo podría cumplirse con “una legislación que adaptara a éstas, en cada caso, a estos nuevos documentos; o que expresamente declarara que los documentos originados en un sistema de tratamiento electrónico de datos, de carácter público, tienen el carácter de instrumentos públicos”.^{293 294}

La Ley 19.799 en su artículo 3, homologa los actos y contratos suscritos por medio de firma electrónica a los celebrados en soporte papel. Sin embargo, en el inciso 2º establece como excepción a dicha homologación, los documentos “en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico”. Así, no es que el legislador se niegue a la existencia de documentos públicos electrónicos, sino que simplemente establece como limitación el que las solemnidades puedan ejecutarse por esta vía.

En conclusión, desde un ámbito estrictamente técnico, es posible celebrar algunos actos y contratos solemnes, y por ende, cumplir con las formalidades necesarias por medios electrónicos.

El problema surge respecto de ciertos actos y contratos solemnes, como por ejemplo los que requieren escritura pública o inscripción en un registro especial. A pesar de que

²⁹² Así se establece, por ejemplo, respecto a los notarios en la Ponencia número 117, del IV Congreso Iberoamericano de Informática y Derecho, Bariloche, 1994, sobre “Resumen Notarial en una contratación por sistema telemático” que brinda la posibilidad de que el notario intervenga en la contratación telemática. Bastaría para ello que el escribano “cuente con servicio de fax o módem interconectado con otra Notaría, a la que acudirá el otro contratante, a quien se transmitirá la oferta por medio informático, y recibirá por igual vía la aceptación, comprometiéndose ambos fedatarios a intercambiarse los respectivos testimonios.” García Rúa, Oscar; Trezza, Alicia y Viacava, Jorge, Escribanos del Colegio de la Capital Federal Argentina, Bariloche, 1994, “La intervención notarial en una contratación por sistema telemático”, citado por Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 75.

²⁹³ Ruiz, Fernando, “El documento electrónico frente al derecho civil y financiero”, op. cit., pág. 78.

²⁹⁴ Así lo señala la Ley 19.052, del 10 de abril de 1991, que otorgó el carácter de instrumento público a los certificados emitidos por sistemas informatizados del Servicio de Registro Civil.

técnicamente ello es plenamente posible, su aplicación requiere de reformas más profundas, a la legislación notarial y registral.²⁹⁵

El artículo 4 también se refiere a los documentos electrónicos con calidad de instrumento público, exigiendo que ellos se suscriban mediante *firma electrónica avanzada*, marcando la diferencia con los de carácter privado y revistiéndolos de autenticidad.

Por último, el artículo 7 efectúa la misma equivalencia de los artículos 3º y 4º, pero orientada a los documentos de los órganos del Estado. De esta manera, los documentos emanados del poder público suscritos por firma electrónica, tendrán pleno valor jurídico, pero para que tengan la calidad de instrumento público o surtan los efectos propios de éste, deberán suscribirse por medio de firma electrónica avanzada.

La ley también se refiere al valor probatorio del documento electrónico que tenga la calidad de instrumento público, tema que será tratado en detalle más adelante.²⁹⁶

• Requisitos del instrumento público electrónico.

La doctrina señala que el instrumento público electrónico debe cumplir con los requisitos del documento público tradicional. Sin embargo, por sus especiales características, tales requisitos deben ser adaptados a esta nueva forma documental.

Así, como primer elemento, se menciona que el documento debe estar revestido de *fehaciencia*. En otras palabras, debe adquirir el carácter de indubitado, sin riesgos, lo que se logra mediante el sistema de autoridad certificadora.²⁹⁷

La Ley 19.799 utiliza a los Prestadores de Servicios de Certificación de firma electrónica acreditadas ante la autoridad competente (la Subsecretaría de Economía, Fomento y Reconstrucción, según el artículo 2 letra e de la Ley y 14 del Reglamento), que autoriza a determinadas personas naturales o jurídicas para actuar como tales. Los

²⁹⁵ El Mensaje del Presidente de la República a la Cámara de Diputados de 9 de Agosto del 2000, al presentar el Proyecto de Ley sobre firma electrónica y los servicios de certificación de firma electrónica, en su pág. 15, señaló que ello era ajeno al proyecto de ley.

²⁹⁶ Cfr. Capítulo II, apartado 5.

²⁹⁷ Así por ejemplo, el *Florida House Bill 1413*, de 30 de Mayo de 1997, permite la participación de los notarios públicos en la autorización de instrumentos electrónicos con firma digital. Mc Bride, Baker & Coles, Summary of legislation relating to digital signatures, electronic signatures and cryptography, edición al 17 de noviembre de 1997 (.///Netscape/ds_sum.htm.), citado por Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 198.

prestadores de servicios emiten los certificados, los que identifican al suscriptor, contienen su llave pública y demás datos acerca del mismo (artículo 15 de la Ley).²⁹⁸

Este requisito, también está consagrado en el artículo 12 letra e del mismo cuerpo legal. Ahí se establece, respecto al otorgamiento de certificados de firma electrónica avanzada (esta clase de firma es necesaria para que los documento electrónicos tengan la calidad de instrumento público según el artículo 4), la obligatoriedad para el prestador de servicios de comprobar *fehacientemente* la identidad del solicitante. Para ello, “el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica”.²⁹⁹

En segundo lugar, se estima que el instrumento público requiere de *seguridad*.³⁰⁰ Ella se obtiene a través de los certificados de firma digital otorgados por los prestadores del servicio, los que en virtud del artículo 2º letra b de la Ley 19.799 dan fe del vínculo entre el firmante y los datos de creación de la firma electrónica.

El último requisito del instrumento público es la *firma*. Como ya se ha adelantado, el artículo 4 de la Ley 19.799 exige que el documento electrónico que tenga el carácter de instrumento público se suscriba por medio de firma electrónica avanzada. Ésta es “aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría”.³⁰¹

²⁹⁸ El legislador chileno se inspiró en la *Digital Signature Act* del estado de Utah (1995), que plantea la misma solución en este aspecto.

²⁹⁹ Ley 19.799, artículo 12 letra e.

³⁰⁰ Este tema se tratará en detalle en el Capítulo III de este trabajo.

³⁰¹ Ley 19.799, artículo 2 letra g.

5. Valor probatorio del documento electrónico.

5.1. Criterios de apreciación de la prueba.

En doctrina se pueden distinguir diversos criterios en torno a la valoración de la prueba. La principal clasificación distingue entre: los sistemas de prueba libre y los de prueba tasada.

En los países en que rige el *principio de la prueba libre o moral*, como en Italia o Argentina, la ley no fija los medios probatorios ni su valor. Por ello, no existe inconveniente en que las partes involucradas en un intercambio de documentos electrónicos produzcan y los jueces acepten como prueba el registro digital de la transacción. Dichos instrumentos, adquieren el mismo valor probatorio del documento escrito, a pesar de que las firmas del emisor y del receptor se efectúen electrónicamente.

En legislaciones que adoptan el *principio de la valoración legal de los medios probatorios o prueba tasada*, como la chilena, los medios de prueba y su eficacia se indican taxativamente en la ley.³⁰²

En este caso puede ocurrir, por ejemplo, que las normas inhiban a los tribunales de utilizar los medios electrónicos como prueba, les impongan expresamente determinada fuerza probatoria, o los admitan sólo cuando faltan otros medios.³⁰³

En conclusión, los documentos electrónicos se admiten espontáneamente como medio de prueba en los sistemas de libre apreciación. En los de prueba tasada sólo es posible su incorporación al sistema probatorio mediante la dictación de una norma que los establezca expresamente.

³⁰² Así, los Códigos Civil y de Procedimiento Civil, en sus artículos 1698 y 341 respectivamente, indican que los medios de prueba son: los instrumentos (públicos o privados), testigos, presunciones, confesión de parte, inspección personal del tribunal y el informe de peritos.

³⁰³ Jijena Leiva, Renato Javier, “Naturaleza jurídica y valor probatorio del documento electrónico. El caso de la declaración de importación electrónica o mensaje CUSDEC”, op. cit., pág. 461.

5.2. Admisibilidad y valor probatorio del documento electrónico en el derecho chileno.

Como se adelantó, en Chile rige el criterio de *la prueba tasada*, esto es, el legislador señala taxativamente los medios probatorios, la forma de rendir la prueba en juicio, y en ciertos casos, su valor.

Las disposiciones generales de tal sistema se comprenden en el Título XXI del Código Civil, que regula la admisibilidad de los medios de prueba y su valor probatorio, y en el Título XI del Libro II del Código de Procedimiento Civil, donde se reglamenta, además de aquéllos, la manera de producir la prueba ante los tribunales.³⁰⁴ Esto sin perjuicio de las normas en materia criminal, señaladas en el Código de Procedimiento Penal.

Sin embargo, el sistema de prueba tasada se aplica de un modo limitado respecto al valor probatorio, traduciéndose en una excepción, admitida sólo cuando la ley lo establece expresamente, como en el caso de la plena fe que se atribuye al instrumento público, al instrumento privado reconocido, o a la confesión judicial sobre un hecho personal.³⁰⁵

Ello debido a que existen situaciones en las que el juez está facultado para apreciar la prueba en conciencia, lo que se traduce en que la regla general para la legislación chilena, respecto a la *valoración de la prueba rendida*, la constituye el sistema de la *libre convicción*, donde el tribunal debe atenerse a los medios de prueba que señala la ley, valorando esos elementos de acuerdo a la convicción que se forme de los hechos.

Una contraexcepción a los casos en que el valor probatorio lo establece la ley, la constituyen las situaciones en que la ley chilena expresamente indica que la prueba se apreciará en conciencia. Esto ocurre, por ejemplo, en materia laboral, donde rige el Título I del Libro IV del Código del Trabajo. También en los juicios de arrendamiento de bienes raíces urbanos y en los seguidos ante los Tribunales de Menores. Pero ello no quiere decir que “la apreciación de la prueba quede entregada al libre arbitrio del juez, sin tener que formarse una entera convicción fundamentada”.³⁰⁶

³⁰⁴ Se trata de los artículos 1698 y siguientes del Código Civil, y al 318 y siguientes del Código de Procedimiento Civil.

³⁰⁵ Herrera Bravo, Rodolfo, “El documento electrónico: algunas vías de aplicación en el Derecho Probatorio Chileno”, op. cit., apartado 2.

³⁰⁶ Ibid.

En conclusión, la valoración de la prueba se rige, por regla general, por la libre convicción, con ciertos matices de prueba legal, atenuada por el legislador en algunos casos, mediante la apreciación en conciencia.

Respecto a los medios de prueba y a la forma en que ella debe ser rendida, la ley los indica taxativamente, siendo el chileno, un sistema de prueba legal.

Todo lo anterior ha llevado al legislador a reconocerle mérito probatorio al documento electrónico a través de diversas disposiciones legales, siendo la más importante la Ley 19.799.

5.2.1. Ley 19.799 y el valor probatorio del documento electrónico.

La Ley 19.799 otorga eficacia probatoria al documento electrónico, a través de su artículo 5º.³⁰⁷

En tal disposición, el legislador distingue entre:

a) Documento electrónico que tiene la calidad de *instrumento público*³⁰⁸, el que hace plena prueba de acuerdo a las reglas generales; y

b) Documento electrónico que posee la calidad de *instrumento privado*, el que a su vez, puede ser:

b.1) Suscrito mediante firma electrónica avanzada.

Hace plena prueba en conformidad a las reglas generales.

b.2) Suscrito por firma electrónica.

Tendrá el mismo valor probatorio de un instrumento privado de acuerdo a las reglas generales.

En este punto conviene recordar, brevísimamente, cuáles son estas “reglas generales” en materia de valor probatorio.

Respecto a los *instrumentos públicos* rige el inciso primero del artículo 1700 y el artículo 1706 del Código Civil, lo que se traduce en que hacen plena fe tanto respecto de

³⁰⁷ El artículo 5 de la Ley 19.799 establece: “Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes: 1.- Los señalados en el artículo anterior (los documentos electrónicos que tengan la calidad de instrumento público, suscritos mediante firma electrónica avanzada), harán plena prueba de acuerdo con las reglas generales, y 2.- Los que posean la calidad de instrumento privado tendrán el mismo valor probatorio señalado en el número anterior, en cuanto hayan sido suscritos mediante firma electrónica avanzada. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales”.

³⁰⁸ Según el artículo 4 de la Ley 19.799 “los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada”.

los declarantes cuanto de los terceros, en lo que respecta a su fecha, al hecho de haberse otorgado y al hecho de haberse efectuado por los interesados las declaraciones que en ellos se consignan. En cuanto a la verdad de estas declaraciones, hacen plena fe sólo contra los declarantes.³⁰⁹

Según el artículo 1702 los *instrumentos privados reconocidos o mandados tener por reconocidos* “tienen el valor de una escritura pública respecto de los que aparecen o se reputan haberlo suscrito, y de las personas a quienes se han transferido las obligaciones y derechos de éstos”. Esto significa, que hacen plena fe en cuanto al hecho de haberse otorgado, a su fecha y en cuanto a la verdad de las declaraciones que en ellos se contenga (artículo 1700 inciso 1).

En consecuencia, los instrumentos privados que no han sido reconocidos, carecen de valor probatorio, por lo que el tribunal, al ponderarlos en una sentencia definitiva, deberá restarles todo mérito, lo mismo que si no se hubieren presentado.³¹⁰

5.2.2. Reconocimiento legal de los documentos electrónicos en otras disposiciones nacionales.

Además de la Ley 19.799, en Chile existen varias disposiciones especiales que se refieren al documento electrónico, otorgándole un carácter de instrumento público o privado.^{311 312}

Entre las normas más importantes se puede mencionar:

a) Código de Procedimiento Penal.

A propósito de la comprobación del hecho punible y la averiguación del delincuente, se encuentran los artículos 113 y 113 bis.

El primero de ellos, establece que siempre que sea necesario para el esclarecimiento de los hechos, el juez podrá valerse de pruebas obtenidas por medios computacionales. Para ello, entre otras medidas, determinará la forma como se dejará constancia en el

³⁰⁹ Casarino Viterbo, Mario, *Manual de derecho procesal. Derecho procesal civil*, op. cit., pág. 111.

³¹⁰ Casarino Viterbo, Mario, *Manual de derecho procesal. Derecho procesal civil*, op. cit., pág. 121.

³¹¹ Todas éstas fueron dictadas con anterioridad a la citada Ley.

³¹² Jijena Leiva, Renato Javier, “Comercio, derecho, firma y documentos digitales o electrónicos”, *Análisis del Boletín N° 2348-07, sobre “Los Documentos Electrónicos”*, op. cit., pág. 38.

proceso de estas pruebas y podrá designar un asesor técnico que desarrolle o explique la prueba.

El artículo 113 bis señala que podrán admitirse como pruebas películas cinematográficas, fotografías, fonografías y otros sistemas de reproducción de la imagen y del sonido, versiones taquigráficas y, *en general, cualquier medio apto para producir fe*. Respecto al valor probatorio, agrega que estos medios podrán *servir de base a presunciones o indicios*.

b) Código de Comercio.

El inciso segundo del artículo 913, ubicado en el Título IV relativo a los sujetos en la navegación y el comercio marítimo, señala que las anotaciones que deben estamparse en el libro bitácora o diario de navegación pueden efectuarse *por medios mecánicos o electrónicos*, siempre que éstos garanticen la fidelidad y permanencia de los datos consignados. El inciso primero indica que tendrá el *valor de un instrumento público* si cumple con los requisitos en él indicados.³¹³

En el artículo 1014 inciso tercero, a propósito de la documentación del transporte marítimo, se establece que la firma en el conocimiento de embarque puede ser registrada por cualquier medio mecánico o electrónico.

c) Código Tributario.

Su artículo 30 inciso 2º dispone que la Dirección puede autorizar a los contribuyentes para que presenten informes y declaraciones en medios distintos al papel, cuya lectura pueda efectuarse a través de sistemas tecnológicos. Para esto se dictó, entre otras, la Resolución N° 4.228, que establece el procedimiento para efectuar la declaración de Impuesto a la Renta a través de Internet.

También se han dictado normas que aluden al *valor probatorio de los documentos tributarios electrónicos*. Sin embargo, se ha preferido otorgar validez legal a las copias impresas en papel, y no a los originales soportados digitalmente.

Así ocurre en el artículo 3º, letra f de la Resolución 1.515, de Abril de 1995, en virtud de la cual las facturas electrónicas sólo tienen existencia legal cuando

³¹³ El artículo 913 inciso primero señala: “El libro bitácora o diario de navegación tiene el valor de un instrumento público, siempre que las anotaciones en él estampadas lleven la firma del oficial de guardia y estén visadas por el capitán de la nave. Estas anotaciones no deben tener espacios en blanco, ni enmendaduras o alteraciones”.

posteriormente a su tramitación, se imprime en un formulario, timbrado en forma previa, un documento que registre el total de las operaciones electrónicas efectuadas en un mes.

Algo similar sucede con el antes mencionado artículo 30 del Código Tributario, el cual una vez que autoriza las declaraciones o informes en medios que puedan leerse por sistemas tecnológicos, señala que la impresión en papel que realice el Servicio de dichos informes o declaraciones, tendrá el valor probatorio de un *instrumento privado* emanado de la persona bajo cuya firma digital se presente.

Por último, el artículo 92 bis del mismo cuerpo legal, relativo a la mantención de los documentos contables, establece que la Dirección está facultada para disponer su archivo en medios diversos al papel que puedan ser leídos tecnológicamente. También señala que el Director puede autorizar a los contribuyentes a mantener su documentación de esta misma forma. Agrega que, la impresión en papel de éstos, tendrá el valor probatorio de un *instrumento público o privado* según sea la naturaleza del original.

d) Convenio sobre Transporte Multimodal de Mercancías.³¹⁴

Su artículo 5 N° 3 establece que la firma de los documentos de transporte multimodal podrá ser registrada por *cualquier medio mecánico o electrónico*, siempre que no sea incompatible con las leyes del país en que se emitan.

e) Ley 18.876, del 21 de Diciembre de 1989, que establece el marco legal para la Constitución y Operación de Entidades Privadas de Depósito y Custodia de Valores.

En el artículo 7, a propósito del contrato de depósito, se indica que entre los depositantes de una misma empresa, las transferencias de valores depositados que sean consecuencia de las operaciones que se efectúen entre ellos, se realizarán mediante cargo en la cuenta de quien transfiere y abono en la del que adquiere, sea sobre la base de una *comunicación escrita o por medios electrónicos* que los interesados entreguen a la empresa. La disposición agrega que “esta comunicación, ante la empresa, será título suficiente para efectuar tal transferencia”.

³¹⁴ Adoptado por las Naciones Unidas el 24 de mayo de 1980 y promulgado por Decreto Supremo N° 380 del Ministerio de Relaciones Exteriores, de 4 de agosto de 1982.

Su artículo 8 señala algo similar respecto a las transferencias en favor de terceros que no sean depositantes en la empresa.³¹⁵

f) Reglamento del Sistema de Pronósticos Deportivos de la Polla Chilena de Beneficencia.³¹⁶

El artículo 9 establece que los pronósticos efectuados por el apostador en el volante serán leídos o captados por medio de los equipos que Polla determine, generándose inmediatamente un registro computacional de la información. De la apuesta realizada quedará constancia en un documento impreso denominado recibo, el que constituye el comprobante y el medio de prueba de la participación del apostador en el concurso.

Por último, se agrega que los registros computacionales de las apuestas son el medio válido para acreditar los pronósticos realizados por el apostador, y que toda anotación o señal que aparezca en el recibo y que difiera de las asentadas en los registros computacionales es nula y de ningún valor.

g) La Ordenanza y otras disposiciones aduaneras.³¹⁷

El artículo 71 inciso segundo de la *Ordenanza de Aduanas* señala que el Director Nacional de Aduanas podrá autorizar que la formalización de las destinaciones aduaneras (que se realiza mediante un documento denominado declaración) se efectúe por medio de un sistema de transmisión electrónica de datos, conforme a las normas que establezca el *Reglamento*.³¹⁸

El artículo 72 agrega que en los casos que se autorice el uso de sistemas de transmisión electrónica de datos, tendrá la calidad de matriz el registro final incluido en el archivo del Servicio, si la correspondiente declaración cumple con las operaciones de presentación, recepción, verificación, aceptación y legalización. Respecto a las copias,

³¹⁵ El artículo 8 de la Ley 18.876 señala: “Las transferencias en favor de terceros que no sean depositantes en la empresa se efectuarán mediante las formalidades propias de la transferencia del dominio, según sea la naturaleza del título de que se trate, con cargo a los valores disponibles que el depositante tenga en cuenta. El depositante comunicará a la empresa por *escrito o por vía electrónica* el nombre del beneficiario. Esta comunicación, ante la empresa, constituirá título suficiente para efectuar tal transferencia”.

³¹⁶ Decreto Supremo N° 114, del 19 de abril de 1989.

³¹⁷ La actual Ordenanza de Aduanas está contenida en el DFL N° 2 de Hacienda, de 1997, que fija el texto refundido, coordinado y sistematizado del DFL 213, de 1953, de dicha ordenanza.

³¹⁸ Corresponde al Decreto Supremo del Ministerio de Hacienda N° 1.015 (de 19 de octubre de 1994), publicado en el Diario Oficial el 11 de febrero de 1995 (modificado por Decreto Supremo de Hacienda N° 139, publicado en el Diario Oficial el 7 de Abril de 2001) y que establece normas en virtud de las cuales el Director Nacional de Aduanas podrá autorizar a los Despachadores de Aduanas para formalizar sus declaraciones mediante un sistema de transmisión electrónica de datos.

se establece que tanto las obtenidas a partir del registro señalado, como las obtenidas de los registros legalizados por el Servicio transmitidos a los agentes de aduanas, se tendrán por auténticas. Además, las primeras tendrán la calidad de instrumento público.

Por otro lado, el *Manual de Procedimientos Operativos para la Transmisión Electrónica de Documentos*³¹⁹ (aprobado por Resolución de la Dirección de Aduanas N° 1.681 de 8 de Abril de 1999 y modificado por la Resolución N° 1.670 de 3 de Mayo del año 2001³²⁰), regula en el N° 6 de su Capítulo I el valor probatorio de los mensajes electrónicos con el Servicio Nacional de Aduanas, y establece que los archivos computacionales de los mensajes “son instrumentos electrónicos que, en caso de conflicto, pueden ser admitidos por los Tribunales de Justicia, de acuerdo con el artículo 72 de la Ordenanza de Aduanas. Para estos efectos, tendrá la calidad de matriz el registro final incorporado al archivo del Servicio Nacional de Aduanas”. En el N° 6 inciso segundo se agrega que, para que los usuarios de Aduana puedan establecer este medio probatorio, deberán poseer “los registros legalizados transmitidos a ellos por el Servicio Nacional de Aduanas, en cuyo caso las copias que se obtengan a partir de estos registros se tendrán por auténticas”. Por último, se añade en el inciso tercero, que en caso de que exista disconformidad entre los datos impresos en los formularios respectivos y la contenida en el sistema computacional del Servicio, deberán proveerse en un medio externo de respaldo e impreso en soporte papel, sin alteraciones ni demoras, copia del registro que les fuere transmitido, y en caso de alegarse destrucción o pérdida de la información, se estará exclusivamente a los datos que se obtengan de los sistemas de respaldo del Servicio, o en su defecto, a los que provea la Red de Valor Agregado.

h) Normas relativas al Banco Central de Chile y a la Superintendencia de Bancos e Instituciones Financieras.

El Número 3, Título VI, del Capítulo III. J.1 del *Compendio de Normas del Banco Central*³²¹, a propósito de los contratos entre operadores de tarjetas y establecimientos comerciales, señala que en el evento que las partes no hubieran precisado cuál es el título o documento que autoriza al negocio afiliado para exigir los pagos respectivos, se

³¹⁹ Cfr. Capítulo III, apartado 7.1.2.1. de este trabajo.

³²⁰ El Subcapítulo III del Capítulo III de la Resolución N° 1.670 fue modificado por la Resolución Exenta N° 4.928 de 28 de Diciembre de 2001.

³²¹ Compendio de Normas del Banco Central, Capítulo III.J.1-1. Normas Financieras. Acuerdo N° 363-04-940721 (Circular N° 3013-204) sobre emisión u operación de tarjetas de crédito.

entenderá que lo es el comprobante de ventas y servicios emitido por el establecimiento y suscrito por el titular de la tarjeta de crédito.

En estas normas se pretende que sean las propias partes, en el ejercicio de la autonomía de la voluntad, las que determinen la naturaleza del título para exigir el pago de las transacciones realizadas o pagadas con tarjetas, pudiendo perfectamente estipularse que lo sea un registro soportado electrónicamente o almacenado en el sistema computacional utilizado para las transacciones.³²² El mismo concepto se contiene en las normativas relativas a las tarjetas de débito,³²³ con las cuales se efectúan operaciones de pago electrónico contra cuentas corrientes bancarias.

5.3. Admisibilidad y eficacia probatoria del documento electrónico en el derecho comparado.

Las necesidades del comercio y de la Administración Pública llevan al establecimiento de normas orientadas a otorgar valor jurídico al documento electrónico en determinadas condiciones.

Como se señaló anteriormente, los ordenamientos jurídicos de los países adoptan distintos sistemas de valoración de la prueba,³²⁴ por lo que la eficacia probatoria del documento digital dependerá del sistema aceptado en cada país.

De esta forma, en los estados en que rige *la prueba libre*, como Dinamarca, el juez es libre para determinar, de conformidad con su íntima convicción, el valor probatorio que puede darse a las pruebas que se presentan. En estos países, existe gran flexibilidad para aceptar todos los medios de prueba, por lo que el documento electrónico no plantea ningún inconveniente.

En cambio, en lugares como España, Portugal o Alemania, es decir, en los *sistemas de prueba legal*, la ley fija los medios de prueba, las condiciones de admisibilidad y la fuerza probatoria. En estos casos, es necesaria una ley especial que dé al documento electrónico valor probatorio.

³²² Jijena Leiva, Renato Javier, “Comercio, derecho, firma y documentos digitales o electrónicos”, *Análisis del Boletín N° 2348-07, sobre “Los Documentos Electrónicos”*, op. cit., pág. 43.

³²³ Compendio de Normas del Banco Central de Chile, Capítulo III.J.2-1. Normas Financieras. Acuerdo N° 571-04- 961219 (Circular N° 3013-278) sobre emisión u operación de tarjetas de débito.

³²⁴ Cfr. Capítulo II, apartado 5.1.

A continuación, se analizará la situación del valor probatorio del documento electrónico en algunos ordenamientos jurídicos.

5.3.1. España.

En el derecho español dos son los cuerpos más importantes que regulan el documento electrónico: la Ley de Enjuiciamiento Civil de 7 de Enero del año 2000 y el Real Decreto-Ley sobre firma electrónica, de 17 de Septiembre de 1999.

La *Ley de Enjuiciamiento Civil*, en su artículo 299, después de enumerar los medios de prueba tradicionales, establece en su segundo apartado, que también se admitirán los medios de reproducción de la palabra, el sonido y la imagen, y también los instrumentos que permiten archivar, conocer o reproducir cualquier dato trascendente para el proceso.³²⁵

Su tercer apartado, abre la posibilidad de admitir otros medios probatorios que pudieran no estar incluidos en el párrafo anterior, con la exigencia de que a juicio del tribunal, se obtenga “certeza sobre hechos relevantes”.³²⁶

De esta forma, el ordenamiento jurídico hispano, *reconoce al documento electrónico como medio de prueba*. Es más, la redacción del artículo es tan abierta que involucra tanto a las actuales tecnologías como a las que están por descubrirse.

Sin embargo, esta ley sólo se pronuncia sobre su admisibilidad, pero nada dice sobre la forma de incorporarlo al proceso ni sobre su valor probatorio.

Respecto al primer problema, es decir, a la manera de incorporar este medio a las actuaciones judiciales, la mayoría de la doctrina afirma que no se trata de una prueba autónoma, por lo que es necesario incluirla en los medios tradicionales establecidos en

³²⁵ El artículo 299 apartado 2º de la Ley de Enjuiciamiento Civil dispone que: “También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso”.

³²⁶ El apartado 3º del artículo 299 de la Ley de Enjuiciamiento Civil señala: “Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias”.

la legislación procesal. Así, su inclusión en el proceso, podría ser a través de la prueba documental, del reconocimiento judicial, o de la prueba pericial.³²⁷

Sobre el *valor probatorio* del documento electrónico, la Ley también guarda silencio. Sólo se refiere, en los artículos 382 y 384, a las reproducciones y a los instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso (es decir, a los señalados en el artículo 299 apartado primero y segundo, pero no a los del tercero) los que serán valorados conforme a las reglas de la sana crítica.

Surgen, entonces, dudas respecto a si la valoración de éstos debe efectuarse conforme a las reglas de la sana crítica, como en el reconocimiento judicial o en la prueba pericial, o siguiendo el valor que establece la ley para las distintas clases de documentos.³²⁸

El *Real Decreto-Ley sobre firma electrónica* incorpora formalmente la firma electrónica al ordenamiento jurídico, al amparo de las discusiones de la Directiva sobre la materia de la Unión Europea.³²⁹

Además de regular la firma electrónica y de reconocer su eficacia jurídica, establece mecanismos de certificación de la misma.

Expresamente se limita la aplicación de sus disposiciones, al señalar que éstas no modifican las disposiciones relacionadas con la celebración, formalización, validez y eficacia de los contratos y actos jurídicos, como tampoco el régimen aplicable a las

³²⁷ Rico Carrillo, Mariliana, “El documento electrónico como medio de prueba”. Ponencia presentada en el Simposio Argentino de Informática y Derecho, 11 y 12 de Septiembre de 2001, Universidad de Buenos Aires, Argentina. <http://elciruelo.freeservers.com/Ponencia11.pdf>, versión html., pág 7.

³²⁸ Así, si se trata de un *instrumento privado*, su validez dependerá de la autenticidad del documento. La firma es la encargada de dotarlos de dicha característica. En el caso de los documentos electrónicos, la firma electrónica avanzada (y no la firma electrónica simple) le otorga un valor jurídico equivalente a la firma manuscrita. Ahora bien, si es un *documento privado reconocido*, tendrá el mismo valor de la escritura pública entre quienes lo hubieren suscrito, constituyéndose en plena prueba. Si el documento, por el contrario, *no es reconocido*, existe la posibilidad de solicitar la prueba pericial a objeto de determinar su autoría y la consiguiente autenticidad del documento. Tratándose de los *documentos públicos*, el juez debe atenerse a las reglas de valoración establecidas para este tipo de documentos. Por último, si en su elaboración ha *intervenido un prestador de servicios de certificación*, certificando la identidad de las partes y el momento en que el documento fue emitido, así como la calidad de los sistemas informáticos utilizados en su creación, el tribunal deberá establecer su valoración de acuerdo a las reglas de la sana crítica. Esto debido a que no se trata de un instrumento público, ya que los prestadores de servicios de certificación no otorgan fe pública, por lo que se trataría de instrumentos privados con características especiales (de ser reconocido por las partes, no existiría ningún problema en el momento de su valoración en tanto que será tomado como una escritura pública, tal como se indicó anteriormente). Rico Carrillo, Mariliana, “El documento electrónico como medio de prueba”, op. cit., pág. 13.

³²⁹ Corporación Tiempo 2 Mil, “Proyecto de Ley que establece normas sobre documentos electrónicos” (Ficha Legislativa N° 989), *Bitácora Legislativa*, Programa de Asesoría Legislativa, Santiago, 20 al 24 de Marzo de 2000, pág.13.

obligaciones.³³⁰ Sus normas, tampoco alteran la normativa que establece las funciones de los individuos facultados, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.³³¹

Sobre su *valor probatorio*, específicamente, establece que la firma electrónica avanzada tendrá en relación a la información consignada de manera electrónica, igual valor jurídico que la firma manuscrita respecto a los datos contenidos en soporte papel y será admitida en juicio, valorándose conforme a los criterios de apreciación señalados en las disposiciones procesales.³³²

Sin embargo, al parecer, el legislador español cae en una impropiedad técnica, ya que lo correcto, desde la perspectiva de la Teoría de la Prueba, sería regular el valor probatorio de los documentos, los que a su vez pueden ser públicos o privados, escritos o no, firmados o no firmados. La firma cumple funciones de identificación del autor del documento, y, autenticación del texto, esto es, vincula al autor con lo expresado, pero la firma no es un medio de prueba en sí misma.³³³

En consecuencia, esta norma, que es anterior en su dictación a la Ley de Enjuiciamiento Civil, debió regular, directamente, los documentos firmados electrónicamente, asimilándolos a alguna de las categorías documentales reguladas en la legislación civil.³³⁴

5.3.2. Italia.

El artículo 116 del *Código de Procedimiento Civil italiano*, consagra el *principio del libre convencimiento del juez*, en virtud del cual el tribunal debe valorar las pruebas

³³⁰ Real Decreto-Ley 14/1999 sobre firma electrónica, artículo 1, apartado 2º.

³³¹ Real Decreto-Ley 14/1999 sobre firma electrónica, artículo 1, apartado 3º.

³³² “La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta, según los criterios de apreciación establecidos en las normas procesales”. Real Decreto-Ley 14/1999 sobre firma electrónica, artículo 3, apartado 1º.

³³³ Pinochet, Olave, “Algunas deficiencias de la nueva legislación sobre firma electrónica y documento electrónico”, Junio 2000. Sitio Web Noticias jurídicas (<http://noticias.juridicas.com/> ; Artículos; Informático), http://noticias.juridicas.com/areas_virtual/Articulos/20-Derecho%20Inform%Etico/200006-fe.htm , apartado “Regulación de la firma electrónica en el Real Decreto Ley”.

³³⁴ Ibid.

propuestas por las partes o por el Ministerio Público según su prudente apreciación, salvo que la ley establezca lo contrario.

Por ello, no existe mayor obstáculo para que las partes produzcan, y para que el juez admita como medios de prueba, los documentos electrónicos, tanto en el proceso civil, penal o administrativo.³³⁵

Sin embargo, en materia civil, rige el principio de la particular eficacia del acto escrito como medio de prueba, por lo que el legislador debió dictar una normativa especial.

Así, el *Reglamento de actos, documentos y contratos en forma electrónica*,³³⁶ Decreto N° 513 de 10 de Noviembre de 1997, trata la eficacia probatoria del documento informático.

En virtud del artículo 5, el documento informático con firma digital tendrá el valor de un documento privado.³³⁷ Asimismo, si el instrumento está revestido de los requisitos establecidos en el presente Reglamento, tendrá la eficacia prevista en el artículo 2712 del Código Civil, es decir, hacen prueba plena del hecho y de las declaraciones que contienen.³³⁸

El artículo 16 efectúa una especial referencia a la intervención del notario, al hablar de firma digital autenticada, teniendo por reconocida a los efectos del artículo 2703 del Código Civil, la firma digital cuya aposición sea autenticada por notario, u otro oficial público autorizado. Este mismo artículo define lo que debe entenderse por autenticación de la firma digital, lo que consistirá en la declaración por parte del funcionario público, de que la firma digital ha sido puesta en su presencia por el titular, previa comprobación de su identidad, de la validez de la clave pública y del hecho de que el documento firmado responde a la voluntad de la parte, y no es contrario al ordenamiento jurídico.³³⁹

³³⁵ Ruiz, Fernando, “El documento electrónico frente al derecho civil y financiero”, op. cit., pág. 92.

³³⁶ El artículo 15.2 de la Ley N° 59, de 15 de Marzo de 1997, autorizó al Presidente de la República a dictar el presente Reglamento.

³³⁷ Según el artículo 2702 del Código Civil, los documentos privados hacen plena fe de la autoría de la declaración, salvo querrela de falsedad, impugnación, no reconocimiento o desconocimiento por parte de la persona contra quien se produce.

³³⁸ Moreno Navarrete, Miguel Ángel, “Hacia una regulación positiva del documento electrónico. El modelo italiano”, España (c 2000, Notaría Digital). Sitio Web Notaría Digital (www.notariadigital.com ; Boletín Digital; Índice Boletín), <http://www.notariadigital.com/boletin.htm> , apartado “El modelo italiano”, letra C.

³³⁹ Ministerio de Justicia Español, “La firma y el comercio electrónico. Aspectos jurídicos de los servicios de la sociedad de la información”, Madrid, 7 de Diciembre de 1999 (c 1998-2003, Asociación de Internautas), Sitio Web Asociación de Internautas (www.internautas.org/ ; Documentos), http://www.internautas.org/documentos/mj_firmacomer.htm#5 , apartado V, letra C, N° 2 (“Legislación Italiana”).

El 8 de Febrero de 1999 el Presidente del Consejo de Ministros dictó el *Decreto que contiene las normas técnicas para la formación, transmisión, conservación, duplicidad, reproducción y validación del documento informático*, en conformidad con la delegación del artículo 3° del Decreto N° 513 de 1997, recién citado.³⁴⁰

5.3.3. Francia.

Sin duda la legislación francesa fue una de las pioneras en esta materia. La *Ley 80/525* del 12 de Julio de 1980 introdujo una modificación en el artículo 1348 del *Código Civil*, por medio de la cual se estableció que el documento electrónico -sin efectuar una referencia textual del mismo- tendría el mismo valor probatorio que el documento en soporte papel, escrito y firmado, cuando cumpliera con los requisitos de inalterabilidad y durabilidad.^{341 342}

Posteriormente, la *Ley N° 2000-230* del 13 de marzo de 2000, sobre adaptación del derecho de prueba a las nuevas tecnologías de la información y relativa a la firma electrónica, estableció cambios al Capítulo IV, sobre la prueba de las obligaciones y del pago, en el artículo 1316 incisos primero al cuarto.³⁴³

A partir de esta reforma también será prueba por escrito aquella que conste en soporte electrónico y esté representada por signos o símbolos dotados de significado inteligible. De esta manera, el escrito electrónico supera la tradicional concepción del escrito asimilado a un soporte físico de papel.³⁴⁴

³⁴⁰ Martino, Antonio A, “Reconocimiento del Valor Jurídico del Documento Digital en Italia: Breve Historia de una Ley”, (c 2000, Notaría Digital). Sitio Web Notaría Digital, (<http://www.notariadigital.com> ; Boletín Digital; Índice Boletín), <http://www.notariadigital.com/boletin.htm> , apartado “Decreto del Presidente del Consiglio dei Ministri 8 de Febraio 1999”, párrafo 1.

³⁴¹ El citado artículo señala: « (...) *Elles reçoivent aussi exception lorsqu’une partie ou le dépositaire n’a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l’original qui entraîne une modification irréversible du support* ».

³⁴² Paladella Salord, Carlos de, “El documento electrónico como prueba-La Reforma del Código Civil Francés”, Septiembre 2000. Sitio Web Carlos de Paladella (<http://comunidad.derecho.org/carlospaladella> ; Artículos propios), <http://comunidad.derecho.org/carlospaladella/cps6.pdf> , pág. 4.

³⁴³ También modificó el artículo 1315, el cual no será analizado en esta ocasión.

³⁴⁴ El artículo 1316 de la Ley N° 2000-230 señala: “La prueba literal, o prueba por escrito, resulta de un seguido de letras, caracteres, cifras o todo otro signo o símbolo dotados de significado inteligible, cualquiera sea su soporte y sus modalidades de transmisión”. « *La preuve littérale, ou preuve par écrit, résulte d’une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d’une signification intelligible, quels que soient leur support et leurs modalités de transmission* ».

Esta disposición permite la prueba mediante la presentación de escritos electrónicos. Sin embargo, éstos deben cumplir con los tres requisitos señalados en el inciso primero:

- a) Identificación del autor del documento;
- b) El proceso de generación del documento debe garantizar su integridad;
- c) El proceso de conservación del documento debe garantizar su integridad.³⁴⁵

En la actualidad los mecanismos criptográficos, entre ellos la firma digital, permiten dar cumplimiento a estas exigencias.³⁴⁶

El sistema francés permite al juez considerar todos los elementos que se aportan en el proceso, cualquiera sea su soporte, con el objeto de determinar los hechos que llevarán a la sentencia. Así lo establece el artículo 1316-2.³⁴⁷

Pero sin duda la norma más importante es el artículo 1316-3, donde se establece una asimilación entre los soportes en que se encuentran los documentos que prueban hechos: contratos, correos electrónicos, ofertas, y todo otro documento en la concepción tradicional del mismo.³⁴⁸ Sin embargo, no se pueden olvidar las exigencias señaladas en el inciso primero de este mismo artículo, para que esta asimilación se produzca de manera incondicional. Es decir, el escrito electrónico es idéntico al soportado en papel sólo cuando cumple las condiciones indicadas en el inciso primero.³⁴⁹

³⁴⁵ Artículo 1316-1: “El escrito en forma electrónica está admitido como prueba con igual fuerza que el escrito en soporte papel, bajo reserva de que pueda ser debidamente identificada la persona de la que emana, y que sea generado y conservado en condiciones que permitan garantizar su integridad”. « *L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».

³⁴⁶ Paladella Salord, Carlos de, “El documento electrónico como prueba. La Reforma del Código Civil Francés”, op. cit., pág. 7.

³⁴⁷ “En el caso en que la ley no haya establecido otros principios, y en defecto de acuerdo válido entre las partes, el juez resuelve los conflictos de prueba literal determinando por cualquier medio el título más válido, cualquiera sea su soporte”. « *Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support* ».

³⁴⁸ “El escrito en soporte electrónico tiene la misma fuerza probatoria que el escrito en soporte papel”. « *L'écrit sur support électronique a la même force probante que l'écrit sur support papier* ».

³⁴⁹ Paladella Salord, Carlos de, “El documento electrónico como prueba. La Reforma del Código Civil Francés”, op. cit., pág. 8.

Por último, en virtud del artículo 1316-4 se equipara la firma ológrafa tradicional y la firma digital, dejando para una norma posterior el establecimiento de los requisitos de carácter técnico que debe cumplir para poder ser admisible en forma perfecta a la primera.³⁵⁰

Esta norma es el *Decreto N° 2001-272* de 30 de Marzo de 2001, que permite la aplicación del artículo 1316-4 del Código Civil y relativo a la firma electrónica.

5.3.4. Estados Unidos.

En el derecho norteamericano se deben tomar en cuenta dos reglas relativas a la presentación en juicio del documento: La Regla de la Mejor Evidencia o “*Best Evidence*” y la Regla de la Prueba por Referencia o “*Hearsay Rule*”. La aplicación de éstas podría llevar, en principio, a la exclusión de los documentos electrónicos como medios de prueba.

Así, la *Best Evidence* obliga al juez a tomar en cuenta sólo la mejor evidencia que pueda presentar la parte, siendo ésta el documento original. En materia electrónica, el documento original es aquel escrito en lenguaje de bits, que sólo puede ser entendido por la computadora, por lo que cualquier otro, de acuerdo a esta regla, no tendría validez jurídica.

Por otro lado, la *Hearsay Rule* sólo admite como medio probatorio al documento, si el autor está presente para prestar testimonio sobre su contenido y para someterse al examen contradictorio. La parte tiene derecho a interrogar al creador del documento, por lo que éste debe conocer su contenido en forma personal. Esta regla podría plantear

³⁵⁰ “La firma necesaria para la perfección de un acto jurídico identifica al que la pone. Manifiesta el consentimiento de las partes a las obligaciones que surgen de ese acto. Cuando la pone un oficial público confiere autenticidad al acto. Cuando es electrónica, consiste en el uso de un procedimiento fiable de identificación que garantiza la conexión con el acto al que se incorpora. La fiabilidad del procedimiento se presume, salvo prueba en contrario, cuando la firma electrónica ha sido creada, la identidad del firmante asegurada y la integridad del acto garantizada en las condiciones fijadas por Decreto del Consejo de Estado”. « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat* ».

inconvenientes cuando existen empresas involucradas, ya que en estos casos, son varias las personas que participan en la elaboración del documento electrónico.³⁵¹

La jurisprudencia, mediante la excepción “*Business Record Exception*”, supone la aceptación del documento electrónico como medio probatorio, “aún sin el testimonio del autor, si se refieren a operaciones propias del curso normal y regular de los negocios, debiendo haber sido registrados en el momento de su conclusión o en un momento inmediatamente posterior”.³⁵²

La *Best Evidence* también se ha adaptado a las nuevas necesidades técnicas y jurídicas. La jurisprudencia, en esta materia, ha señalado que la producción de una copia como prueba del contenido original, es permitida si la parte que se vale de ella demuestra que no ha podido presentar el original, porque éste ha sido destruido luego de su registro informático o “el caso ha sido de registración directa”.³⁵³

En la actualidad, estas ideas están contenidas en la legislación federal, a través de la *Uniform Business Record as Evidence Act*, de la *Uniform Rules of Evidence*, y en las diversas actas estatales sobre firma electrónica (*Electronics Signature Acts*).

Además de éstas, rige el *Common Law*, que autoriza la interpretación adecuada a cada caso de las formalidades que debe cumplir el contrato electrónico, entre las que se encuentra la necesidad de escriturar y firmar los contratos que deben constar por escrito (artículo 2 del Código de Comercio Federal). Respecto de éstos, se ha interpretado que “basta con una reducción intencional a formas tangibles -caso de los documentos electrónicos-, para que se entienda cumplida la exigencia, y teniendo presente que la firma es cualquier signo ejecutado o adoptado por una parte con la intención de autenticar un escrito, concepto dentro del cual queda comprendida la firma electrónica.”³⁵⁴

En definitiva, en el sistema americano, un documento electrónico firmado y de forma tangible, constituye un medio de prueba, incluso respecto de aquellos contratos que deben constar por escrito. Su valor probatorio se determinará en el caso particular.

³⁵¹ Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, op. cit., pág.74.

³⁵² Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 61.

³⁵³ Mariñanski, Flora, “Las nuevas tecnologías y la crisis del documento en soporte papel”. *Revista del Notariado*, N° 817, pág. 480, 1989, Argentina, citado por Ruiz, Fernando, “El documento electrónico frente al derecho civil y financiero”, op. cit., pág.87.

³⁵⁴ Corporación Tiempo 2 Mil, “Proyecto de Ley que establece normas sobre documentos electrónicos”, op. cit., pág. 8.

5.3.5. Inglaterra.

El ordenamiento inglés admite el valor probatorio del documento electrónico en el ámbito civil y penal.

Esto se deriva de la *Criminal Evidence Act* de 1984, la cual consagra condiciones de admisibilidad de los documentos emitidos por ordenadores.³⁵⁵

En el área civil, la *Evidence Act* de 1968 ya incorporaba dentro del concepto de documento, además del clásico documento escrito, los mapas, gráficos, planos, dibujos, fotografías, discos, bandas magnéticas, pistas sonoras y *todo otro mecanismo que permitiera la incorporación del sonido o de los datos para ser reproducidos con o sin ayuda de otros materiales.*³⁵⁶

Pero no fue hasta la *Civil Evidence Act* de 8 de Noviembre de 1995, en que se estableció que ningún documento electrónico puede ser declarado inadmisibile como tal.³⁵⁷ Así, los correos electrónicos y las páginas Web que circulan por la Internet, guardados en la memoria de un computador o de otra manera, constituyen prueba admisible. Lo mismo se aplica a una copia computarizada o a la impresión de documentos electrónicos.

La regla general está indicada por el número 8 del Acta,³⁵⁸ donde se señala que un documento (incluyendo los electrónicos) debe autenticarse de conformidad con las normas que determinen las cortes.

Generalmente, para que un documento sea considerado auténtico, es necesario acreditar su origen, la naturaleza de su obra y la identidad de su autor. También es necesario probar que el sistema electrónico, así como el computador del receptor, operan satisfactoriamente.³⁵⁹

³⁵⁵ Se trata del artículo 69 de la *Criminal Evidence Act*.

³⁵⁶ Ruiz, Fernando, "El documento electrónico frente al derecho civil y financiero", op. cit., pág. 100.

³⁵⁷ De esta forma el Reino Unido deroga la Hearsay Rule que originalmente impedía la admisibilidad de documentos electrónicos como prueba documental. Maldonado Sergio, "Validez transfronteriza de contratos on-line", 2000 (c 2000, Sergio Maldonado), Sitio Web Sergio Maldonado, http://www.smaldonado.com/search/collections/english/evidence_es.htm, apartado "Reglas de "Hearsay": Inadmisibilidad de Documentos Electrónicos como prueba en juicio".

³⁵⁸ "8.-(1) *Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved— (a) by the production of that document, or (b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such manner as the court may approve .-* (2) *It is immaterial for this purpose how many removes there are between a copy and the original*".

³⁵⁹ Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, op. cit., pág. 68.

Sin embargo, el Acta establece que los instrumentos deben ser autenticados a través de un procedimiento, que variará dependiendo de si la parte que somete la evidencia realiza o no negocios de manera ocasional, o pertenece a una autoridad pública.

Así, en el numeral 9, la *Civil Evidence Act* facilita la prueba a comerciantes y autoridades públicas, señalando que sus registros (en sentido amplio³⁶⁰, por lo que se incluyen los digitales) constituyen medios probatorios.³⁶¹ Estos individuos, para probar algo mediante sus registros, deben obtener un certificado emanado de una persona responsable de las actividades que desee probar -por ejemplo un vendedor- “o por el responsable de los registros, atestiguando el hecho de que los documentos electrónicos presentados como evidencia se originan (...) (en) esos registros”.^{362 363}

Si bien a primera vista todos los documentos digitales son admisibles en materia probatoria, su valor ante los tribunales no necesariamente es el mismo, quedando “al arbitrio del juez el ponderar el nivel de autenticidad de tales documentos”.³⁶⁴

5.4. La opinión de los Organismos Internacionales.

5.4.1. Recomendación de Naciones Unidas sobre el valor legal de los registros computacionales (1985).

Las Naciones Unidas (mediante la UNCITRAL), reconociendo la complejidad de adoptar un tratado internacional sobre la materia, ha optado por la adecuación de las normas nacionales como medida práctica.

³⁶⁰ En el párrafo 4° se indica que los registros deben ser entendidos en sentido genérico: “‘records’ means records in whatever form”.

³⁶¹ El número 9 (1) de la *Civil Evidence Act* establece: “A document which is shown to form part of the records of a business or public authority may be received in evidence in civil proceedings without further proof.”

³⁶² Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, op.cit., pág. 68.

³⁶³ El segundo párrafo del número 9 señala: “A document shall be taken to form part of the records of a business or public authority if there is produced to the court a certificate to that effect signed by an officer of the business or authority to which the records belong. For this purpose— (a) a document purporting to be a certificate signed by an officer of a business or public authority shall be deemed to have been duly given by such an officer and signed by him; and (b) a certificate shall be treated as signed by a person if it purports to bear a facsimile of his signature”.

³⁶⁴ Maldonado Sergio, “Validez transfronteriza de contratos on-line”, op. cit., apartado “Reglas de ‘Hearsay’: Inadmisibilidad de Documentos Electrónicos como prueba en juicio”.

Para ello, emitió un importante documento denominado *Legal Value of Computer Records*³⁶⁵ en el que se expresa que las disposiciones relativas a las pruebas concernientes a documentos electrónicos (habla en realidad de expedientes o registros de computadoras) no deben suponer un obstáculo para el uso de las tecnologías emergentes tanto a nivel doméstico como internacional.³⁶⁶

Además, señala que las normas dictadas por los diversos estados deben superar los inconvenientes que surgen de la escritura tradicional, pues incorpora referencias culturales que suponen un freno a su desarrollo.³⁶⁷

5.4.2. Ley Modelo de UNCITRAL sobre Comercio Electrónico.

Como ya se ha señalado, la Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional de 1996 reconoce valor jurídico al documento electrónico.³⁶⁸

El artículo 9, se refiere a la admisibilidad y fuerza probatoria de los mensajes de datos. Así, señala que no se aplicará ninguna norma probatoria que obstaculice la admisión como prueba de un mensaje de datos, por la sola razón de que se trate de un mensaje de datos o por no haber sido presentada en su forma original, siendo aquel mensaje “la mejor prueba que quepa razonablemente esperar de la persona que la presenta”.³⁶⁹

Por último, en el número dos del mismo artículo, se deja claro que para valorar su fuerza probatoria, se debe tomar en cuenta la fiabilidad de la forma en la que se haya conservado la información, la manera en que se identifique al autor y cualquier otra circunstancia relevante.

³⁶⁵ UNCITRAL, “Recomendación en el valor legal de los registros de computadora”, décimo octava sesión, 1985.

³⁶⁶ UNCITRAL, “Recomendación en el valor legal de los registros de computadora”, décimo octava sesión, 1985, N°1 (a).

³⁶⁷ Paladella Salord, Carlos de, “El documento electrónico como prueba. La Reforma del Código Civil Francés”, op. cit., pág. 5.

³⁶⁸ El artículo 5° de la Ley Modelo de UNCITRAL señala que “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.”

³⁶⁹ UNCITRAL, Ley Modelo sobre Comercio Electrónico, artículo 9 N° 1.

CAPÍTULO III.

SEGURIDAD DE LAS TRANSACCIONES MERCANTILES ELECTRÓNICAS.

1. Nociones básicas.

Según se ha indicado con anterioridad³⁷⁰, las transacciones de comercio electrónico pueden efectuarse mediante redes de computadoras *abiertas o cerradas*.

Entre las redes abiertas o públicas, Internet se constituye como la más importante, y es justamente a través de ésta, que tienen lugar la mayoría de los intercambios comerciales electrónicos. Sin embargo, el libre acceso a ella, trae como consecuencia que la información sea fácilmente interceptable.

Por esto, el comercio electrónico realizado a través del Internet requiere de mecanismos tendientes a evitar los problemas que se derivan de la inseguridad propia del medio por donde transitan los datos.

En la actualidad se han desarrollado diversos métodos para proteger la información que se transmite vía redes, siendo el más efectivo, el sistema de *cifrar o encriptar* los datos. Esto se realiza mediante la *criptografía o criptología*, ciencia “que estudia la ocultación, disminución o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones (...)”.³⁷¹

³⁷⁰ Cfr. Introducción, apartado 4.1.3.

³⁷¹ Devoto, Mauricio y Lynch, Horacio M., “Banca, comercio, moneda electrónica y la firma digital”, op. cit., apartado 4.2.

2. Problemas y principios relativos a la seguridad de los mensajes electrónicos.

Un mensaje de datos que utiliza una red abierta de comunicaciones como la Internet puede provocar incertidumbre en torno a determinadas materias.

Así, puede ocurrir que:

- El autor y fuente del mensaje hayan sido suplantados;
- El mensaje sea alterado, de manera dolosa o fortuita;
- El emisor del mensaje niegue haberlo transmitido o el destinatario haberlo recibido;
- El contenido del mensaje sea leído por personas no autorizadas.³⁷²

Éstos y otros riesgos pueden tener lugar en una comunicación electrónica. De ser así, ésta no alcanzaría el grado de seguridad necesario para generar *confianza* en los participantes, la que se traduce en un requisito imprescindible para la expansión y crecimiento del comercio electrónico.³⁷³

Por esto, se estima que los mensajes electrónicos deben cumplir con ciertos *principios indispensables para ser considerados seguros*. Tales son:³⁷⁴

1) La integridad.

Hace referencia al hecho que el contenido del mensaje no haya sido alterado o manipulado durante su envío.

2) La autenticación.

Es la actividad de identificar al autor o remitente de un mensaje de datos.

³⁷² Pérez Pereira, María, “Hacia la seguridad en el Comercio Electrónico”, REDI: *Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., N° 11, Junio 1999 (c 1997-2002, vLex Networks). Sitio Web “vLex”, España (http://v2.vlex.com/global/redi/redi_default.asp), <http://v2.vlex.com/es/ppv/doctrina/fuente.asp?fuelle=29&numero=%2311> , apartado 1 (“Introducción”).

³⁷³ Así lo señaló la Conferencia Ministerial celebrada en Bohn, en Julio de 1997, consagrada en el Dictamen del Comité Económico y Social (CES 1191/97): “un clima de confianza en las transacciones electrónicas constituye la condición sine qua non para desarrollar y expandir el comercio electrónico”. Citado por Pérez Pereira, María, “Hacia la seguridad en el Comercio Electrónico”, op. cit., nota N° 1.

³⁷⁴ Corporación Tiempo 2 Mil, “Algunos Aspectos del Comercio Electrónico y su Regulación” (Tema de Opinión), *Bitácora Legislativa*, Programa de Asesoría Legislativa, Santiago, 15 al 19 Mayo de 2000, pág. 23.

3) El no rechazo o no repudio.

Implica autenticación e integridad. Se refiere tanto al no repudio en origen (que el signatario no pueda negar un mensaje con un determinado contenido) como al no repudio en destino (que el destinatario no pueda negar la recepción de un mensaje con un determinado contenido).

4) La confidencialidad.

Consiste en que la información contenida en el mensaje de datos no sea leída por ninguna persona extraña a la comunicación. Así, sólo el emisor y el receptor tendrán acceso a ella.

Actualmente, la solución tecnológica utilizada para dar cumplimiento a estos requerimientos jurídicos se basa en los *sistemas criptográficos, principalmente en los asimétricos.*

Por ello, se efectuará una breve referencia a la encriptación y a sus diversos métodos, con especial hincapié en los de doble llave o asimétricos. Como se verá, éstos posibilitan, entre otras cosas, firmar electrónicamente un documento, lo que permite identificar a su autor.

3. La encriptación.

3.1. Concepto.

La *encriptación* es el procedimiento a través del cual se transforman mensajes, de manera que resulten ilegibles para personas no autorizadas a tomar conocimiento de ellos. También se conoce con el nombre de *codificación* y deriva del ramo de las matemáticas aplicadas llamado *criptografía*.³⁷⁵

³⁷⁵ Otero Alvarado, Jorge y Lankenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, op.cit., pág.46.

La encriptación se realiza mediante códigos secretos y cifrados que protegen la información, la que sólo puede ser decodificada por quien conoce la clave y una vez que llega a destino.

Así, es posible resolver los problemas de seguridad relativos a la *integridad* y *confidencialidad* del mensaje, más no así los de certeza sobre la *autenticidad* y *el no rechazo*, los que requieren específicamente de las firmas digitales, las que, como se verá, constituyen mecanismos de encriptación más elaborados.³⁷⁶

3.2. Sistemas criptográficos en general.

Los sistemas criptográficos pueden dividirse en dos grandes grupos: los de cifrado simétrico y los de cifrado asimétrico.

3.2.1. Métodos de criptografía simétrica o de clave única.³⁷⁷

Son aquellos que hacen uso de *una clave o llave común* conocida por las partes previamente, y que permite la codificación de los datos, así como su decodificación.

La clave debe ser *secreta*, a fin de evitar que la información caiga en manos de personas no autorizadas a acceder a ella. La seguridad del sistema recae, justamente, en la protección de la clave, ya que el mensaje puede ser descifrado por quien tome conocimiento de ella.

Este sistema puede ser útil para otorgar *confidencialidad* a los datos. Ello debido a que sólo el iniciador y el destinatario del mensaje conocen la clave de acceso. Además, puede brindar *integridad*, ya que si el mensaje ha sido manipulado, al decodificarlo con la clave secreta, éste carecerá de sentido. Por último, puede otorgar *autenticación*, pero sólo *entre las partes*, ya que solamente la otra parte con la que se comparte la clave

³⁷⁶ Jijena Leiva, Renato Javier, “Comercio electrónico y derecho. La problemática jurídica del Comercio Electrónico”, apartado II, 3, nota N° 5.

³⁷⁷ Técnicamente, recibe el nombre de DES (*Data Encryption Standard*), y fue creado por la Agencia Nacional de Seguridad Norteamericana (NSA) en 1977. En un principio se trató de un sistema estandarizado de seguridad para la administración pública. Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 212.

puede haber codificado el mensaje. Sin embargo, no constituye firma, ya que no soluciona la cuestión del no rechazo de origen.³⁷⁸

El secreto de la clave se constituye en el gran inconveniente de estos métodos. La llave debe ser distribuida por medios seguros, con el objeto de evitar que personas no autorizadas tomen conocimiento de ella y manejen la información. Por esto, el uso de una red abierta como la Internet en la distribución de claves, puede resultar peligroso para la seguridad del sistema.

Además, si bien garantizan la *integridad y autenticidad* del mensaje respecto de las partes que comparten la clave, no ocurre lo mismo *respecto de terceros*. Frente a éstos, tanto el signatario como el destinatario, pueden rechazar la autoría del mensaje, atribuyéndolo a la otra parte. Por otro lado, un tercero puede acceder a la clave secreta, y como consecuencia de ello, engañar a una de las partes suplantando a la otra.³⁷⁹

Se ha planteado reforzar este sistema, para lo cual se ha creado la *aplicación Triple DES*. En ésta, el mensaje se encripta dividido en tres bloques, utilizando tres clave diversas. De esta forma, el método simétrico de llave única se transforma en un *sistema de clave múltiple*. Se trata de un sistema más seguro (matemáticamente es mucho más difícil acceder a tres códigos), pero tiene el problema de que implica mayor costo y tiempo.³⁸⁰

3.2.2. Métodos de criptografía asimétrica o de clave doble.³⁸¹

Estos sistemas utilizan *dos claves o llaves complementarias*, asociadas a una única operación criptográfica. Una *clave pública*, accesible a cualquiera, y que sirve para codificar el mensaje; y una *clave privada*, conocida únicamente por su titular y que permite descifrarlo.

³⁷⁸ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.42.

³⁷⁹ Pérez Pereira, María, “Hacia la seguridad en el Comercio Electrónico”, op. cit., apartado 3.1.

³⁸⁰ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 213.

³⁸¹ El método asimétrico de encriptación fue desarrollado en la Universidad de Stanford, California, en 1975 por los matemáticos Whitfield Diffie y Martin Hellman, y aplicado posteriormente por el MIT (*Massachusetts Institute of Technology*) a la firma digital y a los documentos electrónicos.

Así, la información cifrada con una clave pública determinada, sólo puede ser descifrada con la correspondiente clave privada, y viceversa.³⁸²

Ambas llaves se encuentran relacionadas entre sí, a través de algoritmos o funciones matemáticas. En un principio, se trataba de simples cálculos matemáticos derivados, generalmente, de números primos. Hoy, las investigaciones se dirigen a la utilización de curvas elípticas en las técnicas de encriptación.

La *clave privada* debe ser mantenida en secreto, con el objeto que sólo su titular acceda a la información encriptada. Éste accede a ella una vez que el *tercero proveedor del servicio* la elabora y la pone en su conocimiento.

En la práctica, a veces, ni el mismo titular conoce la llave privada, debido a que ella puede contenerse en una tarjeta electrónica (caso en el cual su acceso tiene lugar a través de un PIN o Personal Identification Number), o a través de sistemas biométricos, como el reconocimiento de la voz o de las huellas dactilares.

El sistema asimétrico permite la *confidencialidad*, esto es que el mensaje sea leído sólo por las personas autorizadas para ello. Funciona debido a que el emisor codifica la información a través de la clave pública del destinatario, quien podrá, a su vez, decodificar el mensaje y acceder a los datos con su clave privada. De esta manera, el emisor estará seguro que la información sólo puede ser leída por la persona a quien va dirigido el mensaje.

También permite elaborar *firmas digitales* las que otorgan autenticidad, integridad y no rechazo de origen de los mensajes. En esta situación, la clave privada se usa para elaborar una firma digital y la llave pública para descifrarla.

El emisor de un mensaje (codificado o no a efectos de confidencialidad), lo codifica usando su clave privada, y el receptor lo descifra con la clave pública del suscriptor, de manera que si el mensaje, “conteniendo información textual, es legible, tiene la seguridad de que el mensaje ha sido enviado por el titular de la clave privada correspondiente a la clave pública que él utiliza (*autenticación*)”.³⁸³ También, tiene la certeza que no ha sido alterado (*integridad*), ya que cualquiera que posea la llave pública del usuario puede verificar si el mensaje ha sido modificado, debido a que el criptograma no se decodificará adecuadamente, acusando que ha sido alterado o

³⁸² En la actualidad el sistema de cifrado asimétrico más importante es el que utiliza el algoritmo RSA (Rivest, Shamir, Adleman-nombres de sus gestores).

³⁸³ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 47.

sustituido. Además, el emisor no puede negar ser el autor del mensaje con un contenido determinado (*no rechazo en origen*).^{384 385}

3.2.3. Otras variantes.

3.2.3.1. Métodos híbridos.³⁸⁶

Éstos resultan de la combinación de los sistemas anteriormente expuestos, es decir, utilizan en parte el método simétrico, y en otra el asimétrico.

Así, por ejemplo, el texto de un documento, puede ser codificado con el método de *encriptación simétrica* (también podría utilizarse la variante triple DES) y la clave o la firma electrónica, se cifra con una doble clave (método de *encriptación asimétrica*). De esta manera, el mensaje queda protegido, incluso respecto al rechazo en el envío y en la recepción.³⁸⁷

3.2.3.2. Método asimétrico con utilización de Código Hash. Firma Digital.

Como la aplicación de la criptografía asimétrica sobre todo el documento puede resultar bastante costoso, se ha optado por aplicar al mensaje inicial una *función de hash*, algoritmo que transforma la secuencia de bits en otra menor. Así, se obtiene un resumen del mensaje, llamado *huella digital*, o simplemente, *hash*.³⁸⁸

³⁸⁴ Como se verá más adelante (ver punto 3.2.3.2. del presente Capítulo), al procedimiento de firma puede agregarse la *función hash*, algoritmo que se aplica tanto en la elaboración como en la verificación de la firma electrónica.

³⁸⁵ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 47.

³⁸⁶ Irabien, José Fernando “Key Management y Certificación Digital”, *Revista de Derecho Informático (REDI)*, N° 110, Noviembre 2002 (c1998-2003, Alfa Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/54-5.asp> , párrafo 4°.

³⁸⁷ Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit, pág. 216.

³⁸⁸ El *hash* se caracteriza por ser irreversible, en el sentido que a partir de éste se hace imposible acceder al mensaje inicial completo; y por ser único del mensaje, ya que no es posible obtener un segundo mensaje que produzca el mismo resumen o hash. Así, cualquier modificación en el mensaje produciría un resumen diverso.

Este compendio o hash es codificado asimétricamente, utilizando la llave privada del emisor. Luego, ambos, el mensaje inicial o completo y el hash o resumen cifrado (firma digital) se envían conjuntamente al receptor.³⁸⁹

El destinatario, a quien le han llegado ambos elementos, puede proceder a *verificar la firma digital*. Para ello, decodifica el hash con la clave pública del emisor y aplica la función hash sobre el mensaje completo recibido. Si el hash recibido y decodificado, y el elaborado por el receptor con el mensaje completo recibido son idénticos, el destinatario tendrá la certeza que el mensaje proviene del titular de la clave privada (con lo que se otorga cierta autenticidad), que el contenido del mensaje corresponde al enviado por éste y que no ha sido modificado (integridad).³⁹⁰

Si para dar confidencialidad al mensaje el emisor lo codificó, antes de verificar la firma el destinatario deberá descifrarlo.

El sistema descrito precedentemente, y que parte de la doctrina califica como *firma electrónica*,³⁹¹ resulta útil para resolver los problemas de *integridad y confidencialidad* del mensaje. Sin embargo, éste no es completamente efectivo para asegurar la *autenticación*,³⁹² en la medida que no permite identificar al emisor del mensaje, sino que a un titular de la clave privada. No existe certeza que el par de llaves, que se relacionan matemáticamente, correspondan efectivamente a la persona que se le atribuyen. Como lo indica Apol.lònia Martínez Nadal, “el titular de la clave podría perder el control de la misma”³⁹³ y ser suplantado por otra persona.

Por ello, resulta trascendental solucionar el problema de la distribución segura de las claves, donde adquiere gran relevancia el Certificado Digital y el tercero de confianza que lo otorga: la Entidad Certificadora.³⁹⁴

³⁸⁹ Si además se quiere dar confidencialidad al mensaje (al texto completo o inicial), éste puede ser, a su vez, codificado utilizando el sistema simétrico. La clave única o pública, para que se mantenga secreta entre las partes, necesariamente debe ser comunicada a través de un medio seguro, por lo que puede ser codificada mediante el método asimétrico.

³⁹⁰ Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, *Revista de Derecho Informático (REDI)*, N° 109, Octubre 2002 (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/>; Histórico), <http://www.alfa-redi.org/upload/revista/101502--19-51-publicación.doc>, pág. 7.

³⁹¹ Cfr. Martínez, Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 49; Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, op. cit., pág. 218.

³⁹² Como se señaló, la autenticación es la actividad de identificar al autor o remitente del mensaje de datos. Cfr. Capítulo III, apartado 2.

³⁹³ Martínez, Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 59.

³⁹⁴ Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, op. cit., pág. 7.

En definitiva, por sus resultados, el método asimétrico con utilización de Código Hash es el más utilizado en la actualidad para firmar electrónicamente un mensaje.

4. La firma electrónica.

4.1. Nociones básicas.

Como segundo aspecto dentro del tema de la seguridad, se abordará *la firma electrónica*, que deriva del desarrollo de los sistemas de encriptación de la información tratados precedentemente.

Ella también es fruto de la tecnología, y viene a colaborar en la generación de la confianza requerida para la expansión del comercio electrónico.

En la documentación clásica, *la firma* es necesaria para cumplir determinados propósitos. Tiene un objetivo:³⁹⁵

- Probatorio, vinculando a un individuo con un documento;
- Ritual, destacando la trascendencia del acto entre los sujetos involucrados;
- De expresión del consentimiento, respecto al acto instrumentado; y
- De eficiencia, al transformar en confiable el documento respecto a terceros.

La *firma electrónica* se constituye en el sustituto tecnológico de la firma manuscrita.³⁹⁶ Ésta no sólo imprime un sello personal al documento, que permite identificar al emisor, sino que además, brinda al receptor del mensaje un mecanismo para verificar que el contenido no fue modificado por terceras personas.

Es así como, sobre la base de los *sistemas de encriptación*, es posible “firmar” los mensajes de manera que quienes lo reciban puedan identificar a su autor.³⁹⁷

En la actualidad, la tecnología más utilizada es la *firma electrónica con encriptación asimétrica o de doble clave*.³⁹⁸ Sin embargo, es conveniente tener en cuenta que las

³⁹⁵ Millé, Antonio, “Impacto del Comercio Electrónico sobre la Propiedad Intelectual”, op. cit., pág. 344.

³⁹⁶ Jijena Leiva, Renato Javier, “Comercio electrónico, derecho y firma digital”, *Revista Infoweek*, N° 78, 17 al 6 de Julio de 1999, pág.12.

³⁹⁷ Así se señala en el artículo 2 letra f de la Ley 19.799 que define firma electrónica.

³⁹⁸ Ello ha llevado a algunos autores a hablar de firma electrónica sólo en los casos en que se utilizan métodos asimétricos de cifrado, desconociendo a los simétricos, por su incapacidad de solucionar el problema del no rechazo en origen de un mensaje. Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 43.

legislaciones, en muchas ocasiones, adoptan el principio de *neutralidad tecnológica*, es decir, tienden a regular sólo los efectos de la firma electrónica y no la tecnología usada, ya que ésta evoluciona todos los días.³⁹⁹ Ello ocurre, por ejemplo, en la *Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*, con lo que se intenta evitar su obsolescencia a corto plazo.⁴⁰⁰

4.2. Concepto.

La firma electrónica consiste en una serie de caracteres incluidos en un documento. Es elaborada de acuerdo a procedimientos criptográficos, y lleva un resumen codificado del mensaje, y de la identidad del emisor y receptor.⁴⁰¹

Se caracteriza por ser:

- a) Secreta;
- b) Fácil de producir;
- c) Difícil de falsificar; y
- d) Cambiante en función del mensaje y del tiempo.⁴⁰²

Además permite, entre otras cosas, determinar de manera fiable si las partes intervinientes en una transacción son realmente las que dicen ser, y si el contenido del contrato ha sido o no modificado con posterioridad.⁴⁰³

³⁹⁹ Magliona Markovitch, Claudio Paul, “Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico”, op. cit., apartado 3., letra a).

⁴⁰⁰ Esto es relativo, ya que como se verá, ocurre sólo en algunos aspectos de la ley, como en la firma electrónica (a secas) pero no en la firma electrónica avanzada. Cfr. Capítulo III, 4.6.1. y 4.6.2.

⁴⁰¹ Pouillet, Yves, “Droit de la Preuve: De la liberté aux responsabilités”, texto presentado al coloquio “Informática y Derecho” de Montreal, organizado por la Asociación Quebequesa para el Desarrollo y la Informática Jurídica, citado por Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 70.

⁴⁰² Del Peso Navarro, Emilio, “Los documentos en la era electrónica y su intercambio vía telemática”, IV Congreso Iberoamericano de Informática y Derecho, Bariloche, 1994, citado por Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, op. cit., pág. 70.

⁴⁰³ Ribas, Xavier, “Comercio electrónico en Internet. Aspectos jurídicos”, REDI: *Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., N° 1, Agosto 1998 (c 1997-2002, vLex Networks). Sitio Web vLex, España (http://v2.vlex.com/global/redi/redi_default.asp), http://v2.vlex.com/es/ppv/doctrina/fuente_29.numero_%231 , apartado 5.2.1.

A nivel internacional, la *Directiva Europea 93/1999 sobre firma digital*, define firma electrónica como “los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación”.⁴⁰⁴

En cambio, la *Ley Modelo sobre Comercio Electrónico de UNCITRAL*, si bien no señala claramente un concepto, le reconoce valor, por lo que de su texto se puede colegir que la concibe como aquella que utiliza un método para identificar al firmante del mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos.⁴⁰⁵

4.3. Ventajas de la firma electrónica.

La firma digital implica ciertos beneficios importantes de tener en cuenta. Así:

- a) Es un elemento que asegura la autenticidad del emisor de un mensaje de datos.
- b) Garantiza la integridad del mensaje. Cuando el contenido del documento es modificado, la firma digital se invalida automáticamente, por lo que ella depende del mensaje original.
- c) Es difícil de falsificar, por lo que es más fiable, técnicamente, que la firma manuscrita.
- d) Su utilización por terceras personas sólo es posible con el consentimiento del suscriptor.⁴⁰⁶

4.4. Equivalencia funcional entre la firma digital y la firma manuscrita.

En las distintas legislaciones vigentes, se le reconocen ciertos efectos a la firma digital, los que la equiparan a la manuscrita u ológrafa.⁴⁰⁷

⁴⁰⁴ Directiva Europea 93/1999 sobre firma digital, artículo 2, apartado 1º.

⁴⁰⁵ UNCITRAL, Ley Modelo sobre Comercio Electrónico, artículo 7, Nº 1 letra a).

⁴⁰⁶ Corporación Tiempo 2 Mil, “Algunos aspectos del comercio electrónico y su regulación”, op. cit., pág. 25.

⁴⁰⁷ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 49.

Ello ocurre, por ejemplo, en el artículo 7 de la *Ley Modelo sobre Comercio Electrónico de UNCITRAL*⁴⁰⁸, donde se indica que “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”.⁴⁰⁹

Por su parte, la *Ley de firma digital de Utah* también establece esta equivalencia al consagrar la presunción de que una firma digital tiene el mismo efecto legal que una firma manuscrita si se cumplen con determinados requisitos.⁴¹⁰

El *Reglamento italiano sobre actos, documentos y contratos en forma electrónica de 1997*,⁴¹¹ en su artículo 10.2 también equipara la firma digital sobre un documento informático a la firma escrita tradicional.⁴¹²

Por último, el mismo principio se encuentra en Chile, en la *Ley 19.799*, donde se indica que “la firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales (...)”.⁴¹³

4.5. Sistemas de encriptación utilizados en la firma digital.

En la actualidad se emplean diferentes métodos para firmar digitalmente un documento. Éstos son el resultado de la aplicación de sistemas de encriptación, utilizados para identificar válidamente al emisor del mensaje.

Entre los más fáciles de implementar se puede mencionar el *sistema asimétrico con código hash*.⁴¹⁴ Sin embargo, también se utilizan otros métodos asimétricos de

⁴⁰⁸ Magliona Markovitch, Claudio Paul, “Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico”, op. cit., apartado 3., letra a).

⁴⁰⁹ UNCITRAL, *Ley Modelo sobre Comercio Electrónico*, artículo 7, N° 1.

⁴¹⁰ *Ley sobre firma digital del estado de Utah*, artículo 406, citado por Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 49.

⁴¹¹ Correspondiente al Decreto N° 513 de 10 de Noviembre de 1997, dictado por expresa autorización del artículo 15.2 de la Ley N° 59 de 15 de Marzo de 1997.

⁴¹² Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 50.

⁴¹³ *Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*, artículo 3 inciso 4.

⁴¹⁴ Cfr. Capítulo III, apartado 3.2.3.2. de este trabajo.

identificación del emisor, como el DSS (Digital Signature Standard) y el RSA (derivado del apellido de sus autores, Rivest, Shamir y Adleman).⁴¹⁵

4.6. La firma electrónica en la legislación chilena.

4.6.1. Concepto legal de firma electrónica.

El legislador chileno, en la *Ley 19.799*, define la firma electrónica como “cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor”.⁴¹⁶

La disposición se mantiene neutral desde un punto de vista tecnológico, por lo que no hace mención a ninguna tecnología en particular.

4.6.2. Distinción. La firma electrónica avanzada.

La *Ley 19.799* distingue entre firma electrónica (a secas) y firma electrónica avanzada. Ésta última es “aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría”.⁴¹⁷

Del concepto legal se derivan los *requisitos* que debe reunir la firma electrónica para ser considerada como avanzada. Ésta debe:

- 1) Ser certificada por un prestador de servicios de certificación acreditado;
- 2) Haber sido creada utilizando medios que el titular mantiene bajo su exclusivo control, vinculando la identidad del usuario con la firma;
- 3) Permitir la detección posterior de cualquier modificación o alteración; e

⁴¹⁵ Millé, Antonio, “Impacto del Comercio Electrónico sobre la Propiedad Intelectual”, op. cit., pág. 345.

⁴¹⁶ Ley 19.799 sobre documento electrónico, firma electrónica y servicios de certificación de dicha firma, artículo 2, letra f.

⁴¹⁷ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 2, letra g.

4) Impedir el repudio de la integridad y autoría del documento.⁴¹⁸

Como se puede observar, la firma electrónica avanzada cumple con exigencias adicionales que la transforman en un sistema más seguro que la firma electrónica simple.

Por su seguridad, la legislación le asigna determinados *efectos jurídicos*. Así:

- Para que un documento electrónico tenga la calidad de un instrumento público debe necesariamente suscribirse por medio de firma electrónica avanzada.⁴¹⁹

- Harán plena prueba, en caso de ser presentados en juicio, los documentos electrónicos que tengan la calidad de instrumento público (de acuerdo al punto anterior) y los que posean la calidad de instrumento privado cuando hayan sido firmados mediante firma electrónica avanzada.

Del concepto de firma electrónica avanzada es posible desprender que ella está muy relacionada con la certificación emanada de un prestador de servicios. Es más, la ley los regula extensamente, lo que permite concluir, que en este punto, la *Ley 19.799* tiende a alejarse del principio de neutralidad tecnológica⁴²⁰, dejándolo, como ya se señaló, sólo para la firma electrónica “a secas”.^{421 422}

5. Los Certificados Digitales.

5.1. Planteamiento.

Además de los sistemas criptográficos y de las firmas digitales, resultan fundamentales para el desarrollo de la seguridad de las operaciones efectuadas a través

⁴¹⁸ Fernández Acevedo, Fernando, “Responsabilidad Civil de los prestadores de Servicios de Certificación”, op. cit., pág. 8.

⁴¹⁹ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 4.

⁴²⁰ Se recuerda que la neutralidad tecnológica es un principio en virtud del cual las legislaciones evitan definir determinados estándares tecnológicos, ya que con el avance de la tecnología, la ley puede quedar obsoleta en poco tiempo. Cfr. Capítulo III, apartado 4.1. de este trabajo.

⁴²¹ Un buen ejemplo de una legislación que adopta efectivamente un modelo de neutralidad tecnológica, lo constituye la legislación francesa.

⁴²² Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación,” op. cit., pág. 9.

de la Red, los *Certificados* emitidos por las Autoridades o Entidades de Certificación.⁴²³⁴²⁴

Los certificados tienen por objeto acreditar la identidad del emisor o receptor de un mensaje electrónico. La identificación del sujeto se produce a través del correspondiente certificado, el cual vincula a un suscriptor con una determinada firma electrónica.⁴²⁵ De esta manera, se logra que el receptor del mensaje tenga absoluta certeza de que el emisor del mismo, es realmente quien dice ser.⁴²⁶

Ello otorga mayor fiabilidad a los vínculos establecidos a través de la firma digital, lo que se traduce en un mayor grado de *confianza*, requisito fundamental de toda relación mercantil electrónica.

En cada uno de los estados a nivel mundial la política legislativa determina si estas actividades de identificación las desarrollan entes públicos o privados. Así, pueden ser autoridad certificadora: un órgano estatal, un funcionario dotado de fe pública, un banco respecto a sus clientes, o una empresa particular proveedora de servicios de certificación de firma electrónica.⁴²⁷

5.2. Conceptos y clases de certificados.

Un certificado digital es, en un sentido genérico, un documento electrónico que contiene cierta información, a la que se ha fijado una firma digital por alguna entidad reconocida y en la que confía alguna comunidad de usuarios.⁴²⁸

⁴²³ El término “Autoridad Certificadora” deriva del inglés “*Certification Authority*”, concepto utilizado para individualizar a quien asume (generalmente empresas) la responsabilidad de dar fe y publicitar las claves públicas.

⁴²⁴ También reciben el nombre de “Instituciones de fiabilidad o confianza” o “Autoridades Certificadoras”. Jijena Leiva, Renato Javier, “Comercio electrónico y derecho. La problemática jurídica del Comercio Electrónico”, apartado IV, 2.3.

⁴²⁵ Magliona Markovicth, Claudio Paul, “Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico”, op. cit., apartado 3., letra a).

⁴²⁶ Jijena, Leiva Renato Javier, “Comercio electrónico, derecho y firma digital”, op. cit., pág. 12.

⁴²⁷ Jijena Leiva, Renato Javier, “Comercio electrónico y derecho. La problemática jurídica del Comercio Electrónico”, op. cit., apartado IV, 2.3.

⁴²⁸ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.120.

Diversos autores, y legislaciones como la alemana y la italiana, reconocen *distintas clases de certificados*, los que pueden ser utilizados en objetivos diferentes.^{429 430}

En la actualidad, los certificados más importantes son los que funcionan sobre la base de los sistemas *asimétricos de encriptación*. En este caso, la clave pública se asocia de manera segura a una persona o entidad determinada.

En consecuencia, un certificado que utiliza algoritmos asimétricos es aquel documento electrónico emitido por una Autoridad Certificadora que acredita la correspondencia entre una clave pública y la identidad (u otros atributos) del titular correspondiente, al cual “se añade a una firma electrónica como datos o información característica del firmante para acreditar su identificación o identidad digital (...)”.^{431 432}

En otras palabras, de utilizarse dos claves, una pública y una privada, la seguridad técnica y jurídica estará constituida, como ya se ha explicado, por el hecho que el emisor de la firma utilice *en su elaboración* un sistema de llave criptográfica privada, y en la *verificación* una clave pública asociada. El nexo o vinculación entre el método de verificación de firma y el individuo o suscriptor, se establece con la emisión del certificado otorgado por la Autoridad Certificadora correspondiente.⁴³³

Esta categoría de certificados se convierte, actualmente, en un elemento de carácter sustancial para la aplicación segura de la tecnología de firma electrónica en el ámbito del comercio electrónico. Ello debido a que colaboran en la resolución del problema de

⁴²⁹ La legislación chilena no hace referencia expresa a distintas clases de certificados.

⁴³⁰ Así por ejemplo, la Ley alemana sobre firma electrónica en el párrafo 2 habla del *certificado de clave de firma*, definido como la declaración digital relativa a la atribución de una clave pública a una persona natural y que lleva añadida una firma digital, y de los *certificados de atributos*, constituidos por aquella declaración digital referida inequívocamente a un certificado de clave pública que contiene más información (por ejemplo, datos relativos a la profesión del titular de la firma, o ciertos poderes de representación respecto de una persona natural o jurídica, o la calidad de colegiado, etc.) . El Reglamento italiano, por su parte, reconoce la obligatoriedad del certificador de especificar, a petición del solicitante, y con el consentimiento del tercero interesado, la existencia de poderes de representación o de otros títulos relativos a la actividad profesional o cargos, reconociendo de esta forma los *certificados de atributos*. Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.120.

⁴³¹ Jijena Leiva, Renato Javier, “Comercio, derecho, firma y documentos digitales o electrónicos”, *Análisis del Boletín N° 2348-07, sobre “Los Documentos Electrónicos”*, op. cit., pág. 22.

⁴³² Desde un ámbito jurídico son manifestaciones de voluntad electrónicas, realizadas por una Autoridad Certificadora, que resultan de la verificación que efectúa previamente sobre la autenticidad, veracidad y legitimidad de las claves criptográficas, y de la integridad del documento digital que se firma. Jijena Leiva, Renato Javier, “Comercio, derecho, firma y documentos digitales o electrónicos”, *Análisis del Boletín N° 2348-07, sobre “Los Documentos Electrónicos”*, op. cit., pág. 22.

⁴³³ Jijena Leiva, Renato Javier, “Comercio, derecho, firma y documentos digitales o electrónicos”, *Análisis del Boletín N° 2348-07, sobre “Los Documentos Electrónicos”*, op. cit., pág. 22.

la distribución fiable de llaves públicas (a través de la comprobación de la identidad del titular), propio de las firmas digitales.⁴³⁴

5.3. Elementos personales de los certificados.

Los certificados digitales generan la interrelación de las siguientes personas: la autoridad de certificación, el titular o suscriptor del certificado y el usuario del mismo.

La *Ley 19.799* no se refiere al *usuario del certificado*, distinguiendo sólo entre dos sujetos: el certificador o prestador de servicios de certificación y el usuario o titular, para referirse a la “persona que utiliza bajo su exclusivo control un certificado de firma electrónica”.⁴³⁵ Para efectos de este trabajo, éste se denominará “suscriptor”.

5.3.1. Autoridad de Certificación.

La *autoridad de certificación, entidad certificadora, proveedor de servicios de certificación, autoridad emisora, o certificador* es la “entidad dedicada a la emisión de certificados que contienen información sobre algún hecho o circunstancia del sujeto del certificado”.⁴³⁶

Estas entidades, serán tratadas detalladamente más adelante, por su trascendencia en el tema de la seguridad.⁴³⁷

⁴³⁴ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.122.

⁴³⁵ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 2 letra h.

⁴³⁶ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 122.

⁴³⁷ Cfr. Capítulo III, apartado 6. de este trabajo.

5.3.2. Suscriptor del certificado.

El suscriptor (titular o usuario para la ley chilena) es la persona o entidad, incluida en el certificado, que acepta el certificado.⁴³⁸

En el caso de los certificados de clave pública, tiene legítimamente la clave privada correspondiente a la clave pública que contiene el certificado.⁴³⁹

Dos son las dudas que surgen al hablar del suscriptor de un certificado de firma electrónica: cuál es su naturaleza y cuál es su relación con la autoridad de certificación.

5.3.2.1. Naturaleza del suscriptor del certificado.

En este punto se pretende determinar si el suscriptor del certificado puede ser tanto una persona física como una persona jurídica, o incluso, una entidad sin personalidad. Esto se traduce en la cuestión de si las firmas electrónicas vinculan o no a personas jurídicas.⁴⁴⁰

Si se equipara la firma electrónica a la firma ológrafa, no habría inconveniente en que ambas clases de personas se relacionen mediante una firma digital. Sin embargo, esto no significa que la persona jurídica sea necesariamente titular de un certificado.

En definitiva, este problema puede plantearse en tres formas distintas:

1) Puede pensarse que la persona física sea titular de un certificado con poder de representación de una persona jurídica. Ello ocurre, por ejemplo, cuando una persona física representa a una sociedad.

En esta situación, la firma electrónica de la persona natural que actúa por la sociedad, sería vinculante para la persona jurídica, de conformidad con las normas generales sobre representación y particulares sobre la representación de las sociedades.

⁴³⁸ La Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma define en su artículo 2 letra h al usuario o titular como “la persona que utiliza bajo su exclusivo control un certificado de firma electrónica”.

⁴³⁹ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.137.

⁴⁴⁰ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.138.

El poder de representación podría constar:

- *En el propio certificado* (se trataría de un certificado de atributos). En este caso, las legislaciones que contemplan esta posibilidad exigen una autorización expresa de la persona a quien se representa.⁴⁴¹

- *En el contenido del documento que se firma*. En esta situación, deberá valorarse la eficacia vinculante de tal acto de conformidad con las reglas generales de representación.

Esta primera solución es la más parecida a lo que ocurre tradicionalmente cuando una persona jurídica es representada por una persona natural mediante una firma manuscrita. Sin embargo, cuando el poder consta en el certificado, plantea la dificultad de solicitar la revocación y emisión de un nuevo certificado cada vez que una persona natural deje de ser representante de la persona jurídica.

2) Si se estima que la persona jurídica es titular del certificado, surge el inconveniente de que ella, por su naturaleza inmaterial, no pueda actuar de manera directa. Es decir, no puede firmar materialmente ni a la manera tradicional (manuscrita) ni digital, por lo que de todos modos requiere de una persona física que actúe en su nombre.

3) Por último, si el certificado es emitido por una persona jurídica, indicándose en alguno de los campos opcionales del certificado la persona natural autorizada para firmar materialmente.

Se trata del caso inverso al descrito en el primer punto. Aquél se refiere a una persona natural con poder de representación de una persona jurídica. En cambio, en este caso, el suscriptor del certificado es una persona jurídica la que autoriza a una persona física, para que ponga materialmente la firma de la persona jurídica.

Si bien los resultados de esta solución son idénticos a los planteados anteriormente, lo interesante es que ésta se aleja sustancialmente de la forma en que se vincula una persona jurídica mediante firmas manuscritas: siempre mediante la firma de una persona física. En esta tercera solución, la persona jurídica tiene una firma electrónica propia e independiente de las personas naturales que la representan, lo que resulta imposible en la firma tradicional.

⁴⁴¹ Se trata de ordenamientos como el alemán y el italiano.

En consecuencia, esta solución tiene como ventaja que si el representante no conoce la llave privada y cesa en su cargo, no será necesario revocar y posteriormente emitir un nuevo certificado, sino que bastará con modificar el contenido en la parte relativa a las personas autorizadas para suscribirlo.

En ciertas situaciones, puede resultar aconsejable que la persona jurídica aparezca directamente como suscriptora de un certificado, incluso sin la mención de su representante. Es el caso de situaciones prácticas, en las que no se vinculan a los representantes, sino que simplemente se contrata con una sociedad, como por ejemplo en la autenticación de su página Web o en transacciones pequeñas mediante Internet.

Por todo lo señalado, al parecer, no se requiere una regulación especial respecto de la vinculación de las personas jurídicas por medios digitales. Ni siquiera para que las personas jurídicas sean suscriptoras de certificados digitales.

Las reglas generales de representación bastan para que la firma de una persona con facultades de representación sea vinculante y obligue al representado. Así, desde una perspectiva electrónica, la firma y el certificado de una persona natural con poder de representación serían suficientes para que se obligue una persona jurídica. Incluso, bastaría que en el mismo documento que se suscribe se deje constancia que se actúa en representación de una persona, siendo innecesario que ello conste en el certificado.

De esta forma, se estaría aplicando al ámbito electrónico, la solución planteada en la tradicional escritura sobre papel.

Sin embargo, puede ser importante una regulación especial de las firmas de personas jurídicas en las situaciones indicadas anteriormente, esto es, en las transacciones en que según la contratación tradicional no se identifica al representante ni se examina su poder, por lo que se entiende que se contrata con la persona jurídica. En estos casos, con el objeto que se produzcan idénticos efectos que en la contratación clásica, la persona jurídica deberá aparecer como suscriptora del certificado de forma directa, sin que conste en el certificado el individuo autorizado para utilizar su clave.⁴⁴²

⁴⁴² Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.144.

5.3.2.2. Relación del suscriptor del certificado con la entidad certificadora.

Existen dos clases de relaciones entre una autoridad certificadora y el titular del certificado:

Una relación de *comunidad cerrada*, en la que el certificador y el suscriptor forman parte de una entidad legal o comunidad más o menos amplia, pero cerrada, dentro de la que están destinados a ser usados los certificados. Es el caso, por ejemplo, de la administración pública cuando actúa como autoridad certificadora de sus administrados, o de las asociaciones u organizaciones que certifican a sus miembros.

El objetivo de estos certificados es permitir comunicaciones electrónicas seguras dentro de una misma organización, sin que el hecho que la actuación como autoridad certificadora se transforme en su única labor, y sin que constituya una actividad comercial.

En cambio en la *comunidad abierta*, la autoridad certificadora es una entidad legal ajena e independiente de sus suscriptores, por lo que los certificados se crean para ser utilizados por personas diferentes y fuera del ámbito de la organización certificadora. Es lo que ocurre, por ejemplo, cuando una autoridad certificadora de carácter comercial emite certificados para que ciertos individuos efectúen operaciones electrónicas con terceras personas, las que también actuarán confiando en los certificados emitidos por dicha entidad. En esta comunidad se establece una relación contractual entre el certificador y el suscriptor del certificado, de la que surgen una serie de derechos y obligaciones.

Esta última forma de relacionarse, se constituye en un elemento trascendental para el comercio electrónico seguro, ya que los suscriptores hacen uso de los certificados emitidos por una autoridad para firmar los documentos derivados de las transacciones mercantiles.

5.3.3. Tercero, usuario del certificado.

Es la persona que confía en el certificado.

En los certificados de clave pública, corresponde a la parte que obtiene la clave pública del suscriptor mediante una copia del certificado que para ese suscriptor ha emitido una autoridad de certificación, y que actúa o está en posición de actuar,

basándose en ese certificado y en la clave pública que vincula a una persona determinada (al suscriptor).⁴⁴³

Los usuarios de certificados no poseen, al menos en un principio, una relación contractual directa con la autoridad de certificación. Sin embargo, dependen de ella para su seguridad, ya que para verificar la firma del mensaje electrónico, requieren del certificado emitido por el certificador.

Por ello, es importante distinguirlos del titular o suscriptor del certificado. Además, resulta interesante preguntarse si la autoridad de certificación tiene alguna responsabilidad por los perjuicios que puedan afectar a estos terceros no contratantes que confían en el certificado emitido por dicha entidad.⁴⁴⁴

5.4. Los certificados digitales en la legislación chilena.

5.4.1. Regulación, denominación y concepto de los certificados.

En Chile, los certificados digitales se encuentran reglamentados en el Título IV de la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículos 15 y 16, y en el Reglamento de la misma ley, entre los artículos 28 y 36 inclusive, correspondientes al Título III.

La Ley no efectúa distinción alguna al referirse a los certificados. Habla de los denominados “certificados de firma electrónica” y los define como la “certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica”.⁴⁴⁵

⁴⁴³ Martínez Nadal Apollonia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág.146.

⁴⁴⁴ Como se adelantó, la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma no los menciona.

⁴⁴⁵ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 2, letra b.

5.4.2. Contenido de los certificados.

El artículo 15 de la *Ley 19.799* y el 28 del *Reglamento*, indican las *menciones mínimas* que debe contener un certificado. Éstas son:

a) Un código único que identifique el certificado. Este número permite al tercero que confía en el certificado, consultar, de forma rápida y fácil, el estado de dicho certificado en los registros.⁴⁴⁶

b) La identificación de la entidad certificadora. Ésta consiste en el nombre o razón social, rol único tributario, dirección de correo electrónico, y en caso de estar acreditada, los antecedentes de su acreditación y su propia firma electrónica avanzada.

c) Los datos sobre la identidad del titular, incluyéndose, su nombre, dirección de correo electrónico y su rol único tributario.

d) El plazo de vigencia.

Respecto a los *atributos adicionales* que los certificadores incorporen con el objeto de incorporar límites al uso del certificado, no deben dificultar o impedir la lectura de las menciones anteriormente indicadas, ni su reconocimiento por terceros.⁴⁴⁷

5.4.3. Vigencia del certificado.

5.4.3.1. Vigencia temporal.

Los certificados se caracterizan por tener un período de vigencia, es decir, su validez se encuentra limitada temporalmente. Esto debido a que, entre otras cosas, los prestadores de servicios de certificación verifican constantemente su validez.⁴⁴⁸

El artículo 33 del *Reglamento de la Ley 19.799* se refiere a la *suspensión de la vigencia* de un certificado. Dicha suspensión se produce por la verificación de alguna de estas dos circunstancias:

- La solicitud del titular del certificado; o

⁴⁴⁶ Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, op. cit., pág. 18.

⁴⁴⁷ Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 29 inciso segundo.

⁴⁴⁸ Jijena Leiva, Renato Javier, “Comercio, derecho, firma y documentos digitales o electrónicos”, *Análisis del Boletín N° 2348-07, sobre “Los Documentos Electrónicos”*, op. cit., pág 23.

- La decisión del prestador de servicios de certificación por razones técnicas.

La suspensión del certificado provoca el *cese temporal de sus efectos jurídicos*, de acuerdo con los usos que le son propios, e impide su uso legítimo por parte del titular.

El *fin de tal suspensión* puede producirse por:⁴⁴⁹

a) Decisión del prestador de servicios de certificación de revocar el certificado, en los casos establecidos por la ley.

b) Decisión del prestador de servicios de certificación de levantar la suspensión del certificado, una vez que cesen las causas técnicas que la originaron.

c) Decisión del titular del certificado, cuando la suspensión haya sido solicitado por éste.

El artículo 16 de la *Ley 19.799* señala las *causales que producen que un certificado quede sin efecto*. Tales son:

1) Extinción del plazo de vigencia. Tal término no puede exceder de tres años contados desde su emisión.

2) Cancelación de la acreditación y de la inscripción del prestador en el registro de prestadores acreditados.

3) Cese voluntario de la actividad del prestador no acreditado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador.

4) Revocación practicada por el prestador en alguno de los siguientes casos:⁴⁵⁰

- A solicitud del titular del certificado;

- Por muerte del titular o disolución de la persona jurídica que represente;

- Por resolución judicial ejecutoriada;

- Por incumplimiento de las obligaciones del usuario;⁴⁵¹

- Por las demás causas que convengan al prestador de servicios de certificación con el titular del certificado.⁴⁵²

Los *efectos jurídicos de la revocación* de un certificado se encuentran señalados en el artículo 34 inciso tercero del *Reglamento*. En virtud de tal norma, la revocación

⁴⁴⁹ Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 33.

⁴⁵⁰ Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 34.

⁴⁵¹ Las obligaciones del usuario son las establecidas en el artículo 24 de la Ley 19.799, a saber: Proporcionar la información de su identidad personal u otras circunstancias objeto de certificación, brindar declaraciones exactas y completas, custodiar los mecanismos de seguridad del funcionamiento del sistema y actualizar sus datos en la medida que éstos vayan modificándose.

⁴⁵² Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 34 inciso segundo, letra g.

provoca el cese permanente de los efectos jurídicos del certificado, de acuerdo con los usos que le son propios, e impide el uso legítimo del mismo.

La revocación de un certificado de firma electrónica puede producirse de oficio o a petición de su titular por alguna de las causales enumeradas anteriormente.

En cuanto a la *solicitud de revocación o suspensión*, la ley indica que ella podrá ser dirigida al prestador de servicios de certificación en cualquiera de las formas que establezcan sus prácticas de certificación, y una vez acogida, deberá ser comunicada al titular y publicada en el registro de certificados de acceso público.^{453 454}

5.4.3.2. Vigencia territorial.

Resulta interesante preguntarse si es posible o no aceptar en Chile un certificado digital otorgado por una entidad certificadora radicada en el extranjero.⁴⁵⁵

El artículo 15 inciso 2 de la *Ley 19.799* establece que los certificados de firma electrónica avanzada *pueden ser emitidos por entidades no establecidas en territorio chileno*, siendo equivalentes a los otorgados por prestadores establecidos en Chile. Sin embargo, exige como requisito para ello, que sean homologados por un prestador acreditado, el que será responsable de su homologación, y deberá cumplir con los requisitos fijados en la Ley, el Reglamento o en los convenios internacionales ratificados por Chile y que se encuentren vigentes.

El *procedimiento de homologación* consiste en que el certificador acreditado demuestre a la Entidad Acreditadora que los certificados homologados por éste han sido emitidos por un prestador de servicios de certificación no establecido en Chile, que cumple con ciertas normas técnicas equivalentes a las señaladas en el Reglamento para el desarrollo de la actividad. Efectuada la homologación del certificado de firma electrónica avanzada, el certificador acreditado deberá comunicar tal situación a la

⁴⁵³ La exigencia de publicación es un requisito para que la revocación, suspensión, o en general cualquiera de las causales que ponen fin a la vigencia de un certificado, sean oponibles a terceros. Artículo 36 del Reglamento y 16 inciso tercero de la Ley 19.799.

⁴⁵⁴ Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 36.

⁴⁵⁵ Existen algunas entidades extranjeras que funcionan virtualmente en Chile, como por ejemplo VeriSign, RSA Data Security, ACE, FESTE, etc.

Entidad Acreditadora dentro de tercero día, y se procederá a publicarlo, inmediatamente, en el registro de acceso público.⁴⁵⁶

Las prácticas de homologación, necesariamente, deben estar declaradas en las Prácticas de Certificación.⁴⁵⁷

6. Los Prestadores de Servicios de Certificación.

6.1. Distinción doctrinal. La tercera parte de confianza.

Las transacciones comerciales electrónicas, para ser seguras, requieren de la intervención de una *tercera parte de confianza*.

Una tercera parte de confianza⁴⁵⁸ es cualquier entidad de confianza de las partes intervinientes en una transacción que proporciona servicios de seguridad.⁴⁵⁹

Ésta puede prestar múltiples servicios. Sin embargo, cuando realiza la función específica de emitir certificados se denomina Entidad de Certificación, Autoridad de Certificación, Prestador de Servicios de Certificación, o simplemente, Certificador.

Los *certificados digitales* permiten, entre otras cosas, vincular la identidad de una persona con un determinado par de claves. Así, da fe de la relación entre una clave pública (e indirectamente con la clave privada) y una determinada persona (el titular de la clave pública).^{460 461}

⁴⁵⁶ Se refiere al registro de acceso público establecido en el artículo 7 del Reglamento.

⁴⁵⁷ Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 35.

⁴⁵⁸ En inglés corresponde a las “*Trusted third parties*” o TTP.

⁴⁵⁹ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 64.

⁴⁶⁰ Por su trascendencia en la actualidad, se trata de los que funcionan sobre la base de sistemas asimétricos de encriptación. Cfr. Capítulo III, apartado 5.2.

⁴⁶¹ Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, op. cit., pág. 9.

6.2. Concepto y terminología.

El Prestador de Servicios de Certificación es una “entidad dedicada a la emisión de certificados que contienen información sobre algún hecho o circunstancia del sujeto del certificado (...)”.⁴⁶²

En el caso de los *certificados de clave pública*, es decir, los que asocian un par de claves con una persona concreta, cubren la necesidad de servicios de terceras partes de confianza en el comercio electrónico de los tenedores de pares de claves asimétricas.⁴⁶³ En este caso, cada certificado posee una clave pública y los datos que identifican al titular del certificado.

Como se adelantó en el punto anterior, los diversos organismos y legislaciones a nivel mundial utilizan distintas terminologías para referirse a las terceras partes de confianza emisoras de certificados. Ello, al parecer, depende de la naturaleza de dichas entidades. Así, por ejemplo, con la expresión “autoridad” se otorga un carácter público, mientras que con la denominación “proveedor de servicios de certificación” se concede un matiz más comercial.⁴⁶⁴

La legislación nacional opta por la expresión “Certificador o Prestador de Servicios de Certificación”.⁴⁶⁵

6.3. Naturaleza jurídica.

A nivel doctrinal existe una importante discusión en torno a la naturaleza pública o comercial de las entidades certificadoras, y a su constitución libre o supeditada a la obtención de una autorización previa.

⁴⁶² Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 122.

⁴⁶³ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 122.

⁴⁶⁴ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 123

⁴⁶⁵ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 2 letra c.

Respecto a la primera cuestión, las entidades certificadoras pueden ser *de naturaleza pública o privada*, dependiendo de la opción legislativa de cada estado. También es posible optar entre personas naturales o jurídicas.

En Chile, la *Ley 19.799* establece un sistema mixto, que permite que los prestadores de servicios de certificación sean “personas jurídicas nacionales o extranjeras, *públicas o privadas (...)*”.⁴⁶⁶ Se excluye la posibilidad que la labor certificadora sea efectuada por personas naturales, ya que sólo habla de las personas jurídicas (tanto públicas como privadas con o sin fines de lucro).

A propósito de la *libertad o necesidad de autorización para la constitución* de una entidad certificadora, las diversas legislaciones se inclinan por una u otra. Así por ejemplo, la *Ley de firma electrónica de Utah*, opta por un *sistema con licencia, autorización o acreditación pública*, por el cual la autoridad certificadora debe, necesariamente, cumplir con determinados requisitos, que otorgan mayor credibilidad y uniformidad al uso de firmas digitales.

Esta licencia o autorización establece un marco regulatorio mínimo que genera más confianza en las actuaciones de la autoridad certificadora. Por ello, algunas legislaciones (como la Ley de Utah y el Reglamento italiano) establecen presunciones legales de equivalencia con las firmas manuscritas en favor de las firmas digitales verificadas por referencia a certificados emitidos por una autoridad certificadora autorizada o licenciada.⁴⁶⁷

Sin embargo, estas presunciones han sido criticadas en el sentido que podría entenderse que “suponen la invalidez y/o ineficacia de aquellas firmas digitales verificadas tomando como base certificados emitidos por autoridades sin licencia, o simplemente, la de aquellas firmas verificadas sin la ayuda de certificado alguno”. Por esto, dichas presunciones deben ser entendidas en el sentido de mejorar la confianza de tales firmas digitales, y no de anular la de las certificadas por autoridades no autorizadas o no acreditadas.

El sistema de autorización también puede agregar cierta uniformidad al sistema de firmas digitales. Ello debido que las diversas legislaciones establecen requisitos diferentes para las autoridades de certificación, lo que se traduce en la falta de exigencias comunes en los distintos estados.

⁴⁶⁶ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 11 inciso primero y su Reglamento artículo 2 inciso primero.

⁴⁶⁷ Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, op. cit., pág. 125.

Del artículo 11 inciso primero de la Ley 19.799 y de su relación con el artículo 1° inciso segundo de la misma Ley⁴⁶⁸, se puede deducir que el legislador chileno opta por un *régimen de libre prestación de servicios*, es decir, no exige una autorización previa para la constitución de una entidad certificadora.⁴⁶⁹ Esto sin perjuicio del sistema voluntario de acreditación consagrado en el Título V de la Ley,⁴⁷⁰ por medio del cual se otorga un mayor grado de seguridad a los certificados, transformándose la acreditación, entre otras cosas, en un requisito para certificar firmas electrónicas avanzadas.

6.4. Los Prestadores de Servicios de Certificación en la legislación chilena.

6.4.1. Regulación.

La legislación nacional se refiere a los *certificadores o prestadores de servicios de certificación* en el Título III de la Ley 19.799 (artículos 11 al 14) y en el Título Primero del Reglamento (artículos 2 al 12).

La misma Ley y el Reglamento dedican un Título especial a la *acreditación* de tales entidades. Se trata del Título V (entre los artículos 17 y 22 inclusive) y del Título Segundo (artículos 13 al 27) respectivamente.

6.4.2. Concepto.

La Ley 19.799 define al *Certificador o Prestador de Servicios de Certificación* como la “entidad prestadora de servicios de certificación de firmas electrónicas”.⁴⁷¹

Por su parte, el artículo 11 colabora al señalar que “son prestadores de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que

⁴⁶⁸ El artículo 1 inciso segundo de la Ley 19.799 establece que “Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios (...)”.

⁴⁶⁹ En este punto la Ley sigue el precepto constitucional de la libertad económica (artículo 19 N° 21 de la Constitución Política).

⁴⁷⁰ Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, op. cit., pág. 10.

⁴⁷¹ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 2 letra c.

puedan realizar”.⁴⁷² Este último concepto, permite advertir que en Chile, la actividad certificadora puede ser efectuada por personas jurídicas (excluyéndose a las personas naturales) tanto privadas como públicas, con o sin fines de lucro.⁴⁷³

6.4.3. Clasificación de los prestadores de servicios de certificación.

La Ley 19.799 distingue dos clasificaciones de entidades certificadoras. La primera, divide a los certificadores entre aquellos *domiciliados y no domiciliados en Chile*, y la segunda, entre los *acreditados y no acreditados*.

A continuación se hará referencia a cada una de éstas.

6.4.3.1. Prestador de Servicios de Certificación domiciliado y no domiciliado en Chile.

Desde el punto de vista del domicilio es posible distinguir entre un prestador de servicios de certificación domiciliado en Chile y uno no domiciliado en Chile.

Tal distinción, derivada del artículo 11 inciso 2 de la Ley 19.799, adquiere importancia a la hora de determinar la legislación aplicable y el tribunal competente para resolver los posibles conflictos en los que se vea involucrado el certificador. Además, según el mismo inciso, para que un prestador de servicios de certificación pueda ser acreditado, requiere estar domiciliado en el territorio nacional.

A propósito de esta clasificación, conviene recordar el artículo 15 inciso 2 de la Ley 19.799 que establece que los certificados emitidos por un prestador radicado en el extranjero pueden ser homologados por un prestador nacional.⁴⁷⁴

⁴⁷² Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 11 inciso 1.

⁴⁷³ Cfr. Capítulo III, apartado 6.3.

⁴⁷⁴ Cfr. Capítulo III, apartado 5.4.3.2.

6.4.3.2. Prestador de Servicios de Certificación acreditado y no acreditado.

Como se indicó anteriormente,⁴⁷⁵ el legislador chileno opta por un *sistema de libre prestación de servicios*, en virtud del cual los certificadores no requieren, en ningún caso, de un permiso o autorización para realizar su actividad. Sin embargo, instauró un *régimen voluntario de acreditación*⁴⁷⁶ ante la Subsecretaría de Economía, Fomento y Reconstrucción (denominada Entidad Acreditadora).⁴⁷⁷

De este sistema surgen dos clases de certificadores: *los prestadores de servicios de certificación acreditados y los no acreditados*.

La Ley sólo define, expresamente, a los *prestadores acreditados*, señalando que son “las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en Chile y acreditadas en conformidad (...) (a la Ley y el Reglamento), que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar”.⁴⁷⁸

A diferencia de los no acreditados, éstos se encuentran sometidos a la Entidad Acreditadora, así como también a mayores obligaciones y condiciones “debiendo demostrar la fiabilidad necesaria de sus servicios, garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos, emplear personal calificado, utilizar sistemas y productos confiables que garanticen seguridad, contratar (...) (un seguro de responsabilidad) y contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación”.⁴⁷⁹

La segunda clase de *certificadores, los no acreditados*, pueden efectuar libremente su actividad, aunque quedan sujetos a ciertas obligaciones comunes.

⁴⁷⁵ Cfr. Capítulo III, apartado 6.3.

⁴⁷⁶ Como se verá en el apartado 6.4.6. de este Capítulo, la acreditación es “el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Entidad Acreditadora que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en esta ley y en el reglamento, permitiendo su inscripción en (...)” un registro público. Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 17 inciso primero.

⁴⁷⁷ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 2 letra e.

⁴⁷⁸ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 11 inciso segundo, y Reglamento de la misma ley, artículo 2 inciso segundo.

⁴⁷⁹ Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, op. cit., pág. 15.

6.4.4. Obligaciones de los Prestadores de Servicios de Certificación.

Los certificadores deben tener las capacidades técnicas y económicas, para que la actividad que efectúan proporcione confianza y seguridad a las transacciones que se realizan por medios electrónicos.

Por esto, la *Ley 19.799* y el *Reglamento* contienen ciertas obligaciones que deben ser cumplidas por los prestadores de servicios de certificación.⁴⁸⁰

El artículo 13 de la Ley, establece que el cumplimiento por parte de los *certificadores no acreditados* de las obligaciones indicadas en las letras a),b),c), y j) del artículo 12, adquiere relevancia a la hora de determinar su responsabilidad, ya que será considerado por el tribunal como un antecedente para determinar si existió o no debida diligencia. Esto hace suponer que tales obligaciones son comunes a toda clase de certificadores, en cambio las demás serían propias de los prestadores acreditados.

6.4.4.1. Obligaciones comunes a todo Prestador de Servicios de Certificación.

En primer lugar, se distinguen las *obligaciones dirigidas a otorgar confianza a los titulares o usuarios de los certificados emitidos por los prestadores*, a través de la comunicación de determinada información a los usuarios, como la publicación de las prácticas de certificación y demás procedimientos a seguir en la operación del certificador.⁴⁸¹

En segundo lugar se encuentra la obligación de *mantener un repositorio o registro público*, el cual tiene por objeto verificar los certificados de firma electrónica.⁴⁸²

En tercer lugar, existen las *obligaciones relativas a los mismos certificantes*, como la comunicación del cese de actividad o del traspaso de los datos.

⁴⁸⁰ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 12 y Reglamento de la misma ley, artículos 6 al 12.

⁴⁸¹ S.E. el Presidente de la República, *Proyecto de Ley sobre Firma Electrónica y los Servicios de Certificación de Firma Electrónica*, Cámara de Diputados (Boletín 2571-19), Valparaíso, 22 de Agosto de 2000, pág.22.

⁴⁸² El repositorio se constituye en el pilar fundamental del sistema de firma electrónica, por lo que su eficacia y transparencia son condiciones básicas para la subsistencia del mismo.

Por último, resultan plenamente aplicables a los certificadores ciertas *obligaciones* derivadas de la Ley N° 19.496, sobre *Protección de los Derechos de los Consumidores*, y de la N° 19.628, sobre *Protección de la Vida Privada*.⁴⁸³

Como se señaló, el cumplimiento de estas obligaciones por parte de los certificadores no acreditados, resulta relevante para determinar su responsabilidad.⁴⁸⁴

6.4.4.2. Obligaciones propias de los prestadores de servicios de certificación acreditados.

Estas obligaciones están indicadas, mayoritariamente, en el artículo 12 de la Ley 19.799.

En primer lugar, se encuentra la *obligación de publicar en el sitio de dominio electrónico las resoluciones* de la Entidad Acreditadora que los afecten.⁴⁸⁵

Esta *obligación* lleva implícita la exigencia *de mantener un dominio en la red abierta*, la que está dirigida a favorecer la autorregulación del mercado, a través de la difusión de la información acerca de la forma en que los diversos certificadores llevan a cabo sus actividades.⁴⁸⁶

También está la *obligación de verificar la identidad de los suscriptores*. Para ello, el certificador requerirá, previamente, ante sí o ante un notario público u oficial del registro civil, la comparecencia personal del solicitante o de su representante si se trata

⁴⁸³ De esta manera, el artículo 12 de la Ley 19.799 establece que las obligaciones comunes a todo certificador son: 1) Contar con *reglas sobre prácticas de certificación* que sean objetivas y no discriminatorias, y comunicarlas a los usuarios de manera sencilla y en lengua castellana. 2) Mantener un *registro de acceso público de certificados*, accesible por medios electrónicos de manera continua y regular. En éste quedará constancia de los certificados emitidos y de los que queden sin efecto. 3) Utilizar los datos proporcionados por el titular del certificado sólo para la mantención de dicho registro. 4) Conservar los datos señalados en el número anterior a lo menos seis años, contados desde la emisión inicial de los certificados. 5) Comunicar, a cada uno de los titulares de firmas electrónicas certificadas por ellos, la *cesación voluntaria* en su actividad. Esta comunicación deberá efectuarse con una antelación de a lo menos dos meses al cese efectivo de la actividad. Además, si no hay oposición de dichos titulares, deberán transferir los datos de sus certificados a otro prestador de servicios en la fecha que el cese se produzca. De haber oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. 6) Cumplir con las *demás obligaciones legales*, especialmente las establecidas en esta Ley, en su Reglamento, y en las leyes N° 19.496, sobre Protección de los Derechos de los Consumidores, y en la N° 19.628, sobre Protección de la Vida Privada.

⁴⁸⁴ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 13.

⁴⁸⁵ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 12 letra d.

⁴⁸⁶ S.E. el Presidente de la República, *Proyecto de Ley sobre Firma Electrónica y los Servicios de Certificación de Firma Electrónica*, op. cit., pág. 24.

de una persona jurídica.⁴⁸⁷ Esta exigencia está destinada a evitar que el solicitante del certificado desconozca la autoría del mensaje con posterioridad.

En tercer lugar, se incluye la *obligación de contribuir en la mantención del sistema público de acreditación*, a través del pago de un arancel por la supervisión,⁴⁸⁸ lo que se justifica en que los certificadores se ven beneficiados de la tutela estatal.

Con el objeto de mantener actualizada la información en la Entidad Acreditadora, y para que ésta pueda ejercer su actividad de la mejor manera, se establece la *exigencia de solicitar*, con un mínimo de un mes de anticipo a la cesación de su actividad, la *cancelación de la inscripción en el registro* de prestadores acreditados que lleva la Entidad Acreditadora, y *comunicar a dicha entidad*, el *destino de los datos* de los certificados, especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto.⁴⁸⁹

Asimismo, existe la *obligación del certificador de comunicar a la Entidad Acreditadora cualquier otra circunstancia trascendente que pueda impedir la continuación de su actividad*, especialmente el inicio de un procedimiento de quiebra o que se encuentra en cesación de pagos.⁴⁹⁰

Por último, se establece la *obligación de notificar a cada uno de los usuarios la cancelación de la inscripción en el registro de prestadores acreditados*.⁴⁹¹

Otros artículos de la Ley y el Reglamento también indican ciertas obligaciones exclusivas de los certificadores acreditados.

Así, se encuentra la *obligación de contar con un seguro*, establecido en beneficio exclusivo de los usuarios en su relación con los certificadores⁴⁹² y las *obligaciones que velan por la fiabilidad técnica* del funcionamiento de los prestadores de servicios de certificación.⁴⁹³

⁴⁸⁷ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 12 letra e.

⁴⁸⁸ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 12 letra f.

⁴⁸⁹ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 12 letra g.

⁴⁹⁰ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 12 letra i.

⁴⁹¹ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 12 letra h.

⁴⁹² Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 14 inciso 3 y Reglamento, artículo 12.

⁴⁹³ Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 3.

6.4.5. Responsabilidad civil de los Prestadores de Servicios de Certificación.

La Ley 19.799 se refiere a la responsabilidad de los certificadores en los artículos 13, 14, 15 y 19.

El más importante es el artículo 14, que establece en su inciso primero, que los prestadores de servicios de certificación *responden civilmente* por los daños y perjuicios que resulten de sus servicios de *certificación y homologación*.⁴⁹⁴

Del mismo inciso es posible concluir que el legislador opta por un *sistema subjetivo de responsabilidad*, ya que en su parte final indica que corresponde al prestador de servicios acreditar que actuó con la debida diligencia. Por esto, podría “eximirse de responsabilidad en caso de que acredite que actuó sin culpa, lo cual muestra claramente que se ha optado por el régimen general de responsabilidad establecido en nuestro Ordenamiento Jurídico”.⁴⁹⁵

En este punto, conviene recordar que el artículo 13 alude al hecho que el juez tomará en cuenta como un antecedente para determinar si existió debida diligencia, el cumplimiento de las obligaciones de los prestadores no acreditados de servicios de certificación.⁴⁹⁶

El inciso primero, también, *invierte la carga de la prueba*, ya que a pesar que el legislador no lo señala expresamente, en el hecho se establece una presunción (simplemente legal) de culpa en contra del certificador. Esta figura, se estableció con el objeto de evitar que el tercero que confía en el certificado tenga que probar la culpa del prestador del servicio. Ello resultaría extremadamente difícil, ya que como se sabe, el sistema de certificación utiliza complejos mecanismos técnicos.⁴⁹⁷

⁴⁹⁴ “Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia”. Ley 19.799, artículo 14 inciso 1.

⁴⁹⁵ Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, op. cit., pág. 39.

⁴⁹⁶ Estas son las obligaciones comunes a todo prestador de servicios de certificación, artículo 12 letras a), b), c) y j), tratadas en el punto 6.4.4.1. del presente Capítulo.

⁴⁹⁷ Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, op. cit., pág. 39.

Sin perjuicio de lo anterior, el legislador “protege” a los certificadores mediante dos fórmulas:

1) Consagra una *exención de responsabilidad* para los certificadores por el uso indebido o fraudulento de un certificado de firma electrónica.⁴⁹⁸

2) Permite que los certificadores *limiten su responsabilidad* en cuanto a los posibles usos del certificado.⁴⁹⁹ Ello siempre que el tercero reconozca tales limitaciones.⁵⁰⁰

Con el objeto de cubrir la eventual responsabilidad civil derivada de la actividad certificadora, el legislador establece como obligación de los certificadores acreditados la contratación y mantención de un *seguro* por un monto igual o superior a cinco mil unidades de fomento, tanto para los certificados propios como para los homologados.⁵⁰¹

Este seguro se exige debido a que en la actividad certificadora existen riesgos inevitables, derivados, principalmente, de los rápidos avances en el área tecnológica. Por ejemplo, ataques de terceros en contra de la seguridad que en la actualidad son imposibles, en un futuro próximo podrían ser comunes. Por otro lado, el seguro pretende evitar que los prestadores de servicios de certificación obligados a pagar importantes sumas de dinero, se declaren insolventes, afectando a la comunidad de usuarios de los certificados emitidos por éstos.⁵⁰²

En el último inciso del artículo 14, el legislador descarta que de la responsabilidad por la certificación realizada por un prestador acreditado se derive, a su vez, una *responsabilidad patrimonial para el Estado*.

En esta situación, se estima que la Ley se refiere al hecho en que la Entidad Acreditadora ha sido negligente en la fiscalización de los certificadores acreditados, y a consecuencia de ello, éstos no cumplen con sus exigencias y obligaciones, lo que puede producir perjuicios a un usuario o a un tercero que confía en el certificado. Sin embargo, la constitucionalidad de este inciso es perfectamente cuestionable, debido a que entraría

⁴⁹⁸ El artículo 14 inciso segundo de la Ley 19.799 señala: “Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica”.

⁴⁹⁹ El artículo 14 inciso cuarto indica: “El certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero. El proveedor de servicios de certificación quedará eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado”.

⁵⁰⁰ En consecuencia, respecto a los terceros distintos de los que confían en el certificado, la limitación de responsabilidad no podría operar, dado que se requiere que la cláusula de limitación sea reconocible por éstos, lo que no es posible en este caso, ya que el tercero no tuvo la carga de consultar los datos del certificado.

⁵⁰¹ Artículo 14 inciso tercero de la Ley 19.799 y 12 del Reglamento.

⁵⁰² Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, op. cit., pág. 40.

en contradicción con el artículo 38 inciso 2° de la Constitución, el cual no establece la posibilidad de eximir de responsabilidad extracontractual al Estado mediante una ley.⁵⁰³

6.4.6. Acreditación de los Prestadores de Servicios de Certificación.⁵⁰⁴

6.4.6.1. Concepto.

La *acreditación* es el procedimiento por el cual el prestador de servicios de certificación demuestra a la *Entidad Acreditadora* que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos establecidos en la Ley 19.799 y en su Reglamento, permitiendo su inscripción en un registro público.⁵⁰⁵

En virtud de lo establecido por el artículo 2 letra e de la Ley 19.799 y por el 14 del Reglamento, en Chile, las funciones de la Entidad Acreditadora son realizadas por la *Subsecretaría de Economía, Fomento y Reconstrucción*.

6.4.6.2. Importancia de la Acreditación.

Si bien en Chile la acreditación es *voluntaria*, ella adquiere una importancia fundamental, toda vez que para que exista una firma electrónica avanzada debe haber un prestador acreditado que la certifique.⁵⁰⁶

⁵⁰³ Fernández Acevedo, Fernando, Responsabilidad Civil de los prestadores de Servicios de Certificación, op. cit., pág. 40.

⁵⁰⁴ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, Título V.

⁵⁰⁵ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 17 y Reglamento, artículo 13.

⁵⁰⁶ Se recuerda que según el artículo 2 letra g de la Ley 19.799, firma electrónica avanzada es “aquella certificada por un prestador acreditado (...)”.

6.4.6.3. Requisitos del Prestador de Servicios de Certificación para ser acreditado.

El prestador de servicios de certificación, para ser acreditado, debe dar cumplimiento a una serie de condiciones señaladas en la ley.

La evaluación del cumplimiento de tales condiciones corresponde a la Entidad Acreditadora, de acuerdo con las normas técnicas aplicables a la prestación del servicio, en el proceso de acreditación.⁵⁰⁷

Las exigencias referidas son:⁵⁰⁸

- 1) Demostrar que sus servicios son fiables;
- 2) Garantizar un servicio seguro de consulta del registro de certificados emitidos;
- 3) Utilizar personal calificado para la prestación de los servicios ofrecidos;
- 4) Emplear sistemas y productos confiables que garanticen la seguridad en la certificación;
- 5) Contratar un seguro de responsabilidad civil equivalente a cinco mil unidades de fomento como mínimo; y⁵⁰⁹
- 6) Poseer tecnología suficiente para desarrollar la actividad de certificación.

6.4.6.4. Procedimiento de acreditación.⁵¹⁰

El procedimiento de acreditación de un prestador de servicios de certificación comienza con una *solicitud* que se presenta a la Entidad Acreditadora. Ella debe individualizar claramente al interesado, indicando:

- Nombre o razón social;
- RUT;
- Nombre y RUT del representante legal;
- Domicilio social;

⁵⁰⁷ Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 17 inciso segundo.

⁵⁰⁸ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 17 inciso segundo y Reglamento artículo 17 inciso primero.

⁵⁰⁹ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 14 inciso tercero.

⁵¹⁰ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 18 y Reglamento artículos 18 al 22.

- Dirección de correo electrónico; y
- Aceptación expresa de dicho medio electrónico como medio de comunicación.

Tal solicitud debe ir acompañada de ciertos *documentos*:

- Del comprobante que acredita el pago de los costos de la acreditación; y
- De los antecedentes que permitan verificar el cumplimiento de las condiciones de acreditación, tratados en el punto anterior, con excepción de la póliza de seguro.

Una vez que la Entidad Acreditadora recibe la solicitud, dentro del quinto día hábil, deberá *verificar su admisibilidad* a través de la evaluación de los antecedentes requeridos.

Si la solicitud es *declarada inadmisibile*, el interesado debe ser informado dentro de tercero día hábil para que complete los antecedentes dentro de los quince días siguientes, bajo apercibimiento de tenerse por rechazada la solicitud.

Ahora bien, si la solicitud es *admitida a trámite*, la Entidad Acreditadora procederá a efectuar un *examen sobre el cumplimiento de los requisitos y obligaciones* exigidos por la Ley y el Reglamento para obtener la acreditación (se trata de los señalados en el artículo 17 de la Ley 19.799).⁵¹¹ Para esto, puede incluso contratar expertos.⁵¹²

Si el interesado cumple con los requisitos y obligaciones para ser acreditado, se procede a *certificar* el hecho y que cuenta con un plazo de veinte días para acompañar la póliza de seguros, bajo apercibimiento de tenerse por rechazada la solicitud. Para dicha certificación, la Entidad Acreditadora dispone de noventa días contados desde la fecha de la admisibilidad de la solicitud, prorrogables por una vez y por motivos fundados.

En el evento que la Entidad Acreditadora estime que el prestador de servicios de certificación *no cumple con las normas técnicas* fijadas para el desarrollo de la actividad, indicará si los incumplimientos tienen o no el carácter de subsanables, y si afectan o no el correcto funcionamiento del sistema y de los fines previstos en la Ley para la firma electrónica avanzada.

En este punto, la actuación de la Entidad Acreditadora dependerá de los incumplimientos, así:

- *Si no son subsanables*, procederá a dictar una resolución por la cual rechaza la solicitud de acreditación.

⁵¹¹ Cfr. Capítulo III, apartado 6.4.6.3. de este trabajo.

⁵¹² Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 18 inciso segundo.

- Si son subsanables y no alteran el correcto funcionamiento del sistema ni de los fines previstos en la Ley para la firma electrónica avanzada, procederá a acreditar al interesado, previa autorización de un plan de medidas correctivas.

Completados los requisitos, el interesado deberá solicitar que se *certifique que la solicitud se encuentra en estado de resolverse*. Con dicha certificación comienza a correr un plazo de veinte días para que la Entidad Acreditadora proceda a acreditar al solicitante.⁵¹³

6.4.6.5. Efectos de la acreditación.⁵¹⁴

La acreditación de un prestador de servicios de certificación produce importantes efectos, tales como:

- 1) La inclusión en un *registro público de prestadores acreditados* que lleva la Entidad Acreditadora;
- 2) Autoriza al certificador para emitir *certificados de firma electrónica avanzada*;
- 3) El certificador es sometido a la *inspección* de la Entidad Acreditadora;
- 4) Los demás efectos que señale la Ley y el Reglamento.

6.4.6.6. Cesación de la acreditación y cancelación de la inscripción.⁵¹⁵

La Entidad Acreditadora está facultada para *dejar sin efecto la acreditación* mediante resolución fundada. Dicha resolución debe ordenar, además, la *anulación de la inscripción* en el registro público de prestadores acreditados.

⁵¹³ Si el interesado denuncia el incumplimiento de dicho plazo ante la misma entidad y ésta no se pronunciare dentro del mes siguiente, la solicitud se entenderá aceptada. Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 18.

⁵¹⁴ Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 23.

⁵¹⁵ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 19 y Reglamento, artículos 25 al 27 inclusive.

La ley señala expresamente las *causales de cesación de la acreditación*. Ellas son:

- 1) La solicitud ante la Entidad Acreditadora del prestador acreditado;⁵¹⁶
- 2) La pérdida de las condiciones que fundamentaron su acreditación, la que será calificada por trabajadores o peritos de la Entidad Acreditadora, de acuerdo con su facultad de inspección; y⁵¹⁷
- 3) El incumplimiento grave o reiterado de las obligaciones que establece la Ley y el Reglamento.

Respecto a las dos últimas causales enumeradas, el certificador tendrá cinco días hábiles para efectuar sus *descargos*.

Presentados éstos ante la Entidad Acreditadora, ella deberá evacuar su *resolución* dentro de los 15 días siguientes, plazo prorrogable por el mismo período y por motivos fundados.

El interesado posee dos instancias para reclamar de esta resolución de la Entidad Acreditadora. Una *administrativa*, que se efectúa ante el Ministro de Economía, Fomento y Reconstrucción, dentro de los cinco días contados desde su notificación. En ésta, el ministro cuenta con treinta días para resolver. También existe una *reclamación jurisdiccional* para ante la Corte de Apelaciones correspondiente a su domicilio, a la que es posible recurrir dentro de los diez días siguientes a la fecha en que se notifique la resolución que dicte el ministro, o en su caso, desde que se certifique que la reclamación administrativa no fue resuelta dentro de plazo.⁵¹⁸

Por último, los prestadores de servicios de certificación tienen la *obligación de comunicar la cancelación de la inscripción* a los titulares de firmas electrónicas certificadas por ellos. Además, la propia Entidad Acreditadora publicará un aviso en un medio de prensa escrito de circulación nacional, a costa del certificador, que tiene por objeto informar la cancelación de la inscripción.

⁵¹⁶ Para que la solicitud se haga efectiva debe ser presentada con a lo menos un mes de anticipación a la fecha del término previsto por el prestador de servicios de certificación acreditado. Además, tiene que señalar el destino que se dará a los certificados y a los datos de ellos, comunicando tal situación a los titulares de los certificados emitidos, indicando que de no oponerse se transferirán los certificados a otro prestador de servicios de certificación. También debe garantizarse el pago de una publicación dando cuenta de la cancelación, de acuerdo al artículo 27 de la Ley 19.799.

⁵¹⁷ Cfr. Capítulo III, apartado 6.4.6.7. de este trabajo.

⁵¹⁸ Esta reclamación jurisdiccional ante la Corte de Apelaciones tiene importantes características indicadas por el artículo 19 inciso segundo. Tales son: 1) La reclamación debe ser fundada; 2) Su agregación en tabla, vista y fallo se rige por las normas del recurso de protección; y 3) Contra la resolución no procede recurso alguno.

Los certificados sólo quedan sin efecto a contar de la fecha de publicación del aviso, a menos que los datos de los titulares hayan sido transferidos a otro proveedor del servicio acreditado.

6.4.6.7. Facultad Inspector de la Entidad Acreditadora.⁵¹⁹

La Entidad Acreditadora puede ejercer la facultad de inspeccionar a los prestadores de servicios de certificación acreditados. Mediante dicha facultad, velará por la observancia de:

- Las condiciones requeridas para otorgar la acreditación; y de⁵²⁰
- Las obligaciones de los certificadores durante la misma.⁵²¹

La facultad inspectora comprende *la inspección ordinaria* y *la extraordinaria*. La primera se refiere a la facultad de efectuar una visita anual a las instalaciones del certificador acreditado, además de solicitar, semestralmente, información sobre el desarrollo de la actividad. La segunda, es ordenada por el Subsecretario mediante resolución fundada, y se realiza de oficio o por denuncia motivada sobre la prestación del servicio.

Los funcionarios o peritos habilitados por la Entidad Acreditadora, para ejercer su función, pueden requerir al prestador de servicios de certificación *información adicional* a la proporcionada por él, la que debe ser suministrada dentro del quinto día contado desde la solicitud, sin perjuicio del otorgamiento de plazos especiales dependiendo del tipo de información.

⁵¹⁹ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 20 y Reglamento artículo 15.

⁵²⁰ Cfr. Capítulo III, apartado 6.4.6.3 de este trabajo.

⁵²¹ Cfr. Capítulo III, apartado 6.4.4.2. de este trabajo.

6.4.6.8. Registro Público de Prestadores de Servicios de Certificación acreditados.

Como se adelantó, la Entidad Acreditadora debe llevar un registro público de certificadores acreditados, en el cual deben constar determinados datos señalados en el Reglamento.⁵²² Tales son:

- 1) El número de la resolución que otorga la acreditación;
- 2) El nombre o razón social del certificador;
- 3) La dirección social;
- 4) El nombre del representante legal;
- 5) El número de teléfono;
- 6) El sitio de dominio y correo electrónico;
- 7) La compañía con que se contrató la póliza del seguro de responsabilidad.

7. Regulación relativa a la Seguridad del Comercio Electrónico.

A nivel mundial, sólo en 1995 comenzó la *regulación legal de los sistemas de seguridad del comercio electrónico, especialmente de la firma electrónica*. El estado norteamericano de Utah fue el primero en dictar una normativa al respecto, la que se ha convertido en modelo para las posteriores legislaciones, incluidas entre ellas la chilena.

En la actualidad, la mayoría de los países, incluidos Chile, cuenta con leyes que tratan la seguridad del comercio realizado a través del Internet. En la mayor parte de los casos, la firma electrónica, los certificados y los prestadores de servicios de certificación se plantean como la solución al problema de la seguridad.

⁵²² Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, artículo 16.

7.1. La Ley chilena.

7.1.1. La Ley 19.799⁵²³ y el Reglamento.⁵²⁴

Como se ha indicado en reiteradas ocasiones, la Ley 19.799 y su Reglamento constituyen la piedra angular de la legislación nacional en materia de seguridad del comercio electrónico.

La seguridad, necesaria para el fomento del comercio, sólo es posible mediante el desarrollo de distintos sistemas o productos, entre los que se cuenta, actualmente, la firma electrónica, los certificados y los prestadores de servicios de certificación.

Ambas disposiciones reconocen y regulan legalmente tales sistemas.⁵²⁵

7.1.2. Otras disposiciones nacionales.

Además de la Ley 19.799 y su Reglamento, en el ordenamiento jurídico chileno se pueden encontrar otras disposiciones que contienen reglas relacionadas con la seguridad. Algunas de ellas son anteriores, en su dictación, a la Ley 19.799.

En general, se trata de normas que regulan la seguridad electrónica para ámbitos específicos, como el aduanero y el tributario.

7.1.2.1. Normativa aduanera.

Gran importancia adquiere el tema de la seguridad electrónica en el ámbito aduanero. Por ello, la autoridad, junto con establecer una regulación que permite reconocer las actuaciones electrónicas con el Servicio Nacional de Aduanas, establece procedimientos operativos para la transmisión electrónica de documentos, y considera

⁵²³ Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, promulgada el 25 de Marzo de 2002 y publicada en el Diario Oficial el 12 de Abril del mismo año.

⁵²⁴ Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, aprobado por D. S. N° 181 del Ministerio de Economía, Fomento y Reconstrucción, el 9 de Julio de 2002 y publicado en el Diario Oficial el 17 de Agosto del mismo año.

⁵²⁵ Al abordar la firma electrónica, los certificados y los prestadores de servicios de certificación, se analizó el tratamiento dado a cada uno de ellos en la Ley 19.799 y en su Reglamento. Cfr. Capítulo III, 4.6., 5.4., 6.4. de este trabajo.

normas para la protección de la información involucrada en dichas transmisiones y trámites.

a) Manual de Procedimientos Operativos para la Transmisión Electrónica de Documentos y sus Anexos.⁵²⁶

Esta disposición establece reglas aplicables a cualquier flujo de información desde y hacia el Servicio Nacional de Aduanas que se efectúe mediante transmisión electrónica de datos, relacionado con el ingreso o egreso de mercancías al o del territorio chileno. Incluye, de manera especial, las disposiciones relativas a los diferentes documentos (destinaciones aduaneras, por ejemplo) que entregan la información exigida por Aduanas.⁵²⁷

En una primera parte, define varios términos relacionados con la seguridad, como certificado digital, encriptar, firma electrónica y prestador de servicios de certificación. Luego, en el Capítulo II, dedicado a los usuarios conectados al Servicio Nacional de Aduanas, se establecen los diversos requisitos que debe cumplir la conexión del usuario, tanto a través de Internet, de una Red de Valor Agregado, o en forma directa. En los tres casos se exige que tal conexión cumpla con las medidas de seguridad, las que tienen por objeto dar confiabilidad a la transferencia electrónica de datos entre el emisor y el receptor del mensaje.

Sin embargo, la principal normativa relacionada con el tema de la seguridad se encuentra en el *Subcapítulo III del Capítulo III*, modificado, en esta parte, por la *Resolución Exenta de la Dirección Nacional de Aduanas N° 4.928* de 28 de Diciembre de 2001, y que regula a las entidades de certificación digital.

La Resolución Exenta N° 4.928 establece *el uso de la firma electrónica* para los documentos y trámites que se efectúan ante y desde el Servicio Nacional de Aduanas por medio de una transmisión electrónica de datos a través de las redes públicas de Internet.⁵²⁸

⁵²⁶ La Resolución del Director Nacional de Aduanas N° 1.681 de 8 de Abril de 1999 fijó el texto refundido del Manual de Procedimientos Operativos para la Transmisión Electrónica de Documentos y sus Anexos. Éste ha sido modificado por la Resolución N° 1.670 de 3 de Mayo de 2001 (que reemplaza los Capítulos I al V e incorpora los Anexos N° 8 al 12) y por la Resolución Exenta N° 4.928 de 28 de Diciembre de 2001 (que modifica el Subcapítulo III del Capítulo III). Cfr. Capítulo II apartado 5.2.2. letra g, de este trabajo.

⁵²⁷ Manual de Procedimientos Operativos para la Transmisión Electrónica de Documentos y sus Anexos, modificado por la Resolución N° 1.670 de 3 de Mayo de 2001, Capítulo I, N° 1, inciso primero.

⁵²⁸ Resolución Exenta N° 4.928 de la Dirección Nacional de Aduanas, de 28 de Diciembre de 2001, N° 1.

Además, señala que para que los usuarios del Servicio Nacional de Aduanas puedan actuar válidamente en una transmisión electrónica de datos con firma electrónica, deberán tener un certificado de firma electrónica emanado de una *Entidad Certificadora aceptada por el mismo Servicio*.⁵²⁹

En consecuencia en este caso, y a diferencia de la Ley 19.799, la aceptación o acreditación de un certificador es competencia del Servicio Nacional de Aduanas y se constituye en un requisito sin el cual el certificador no puede otorgar certificados válidos en materia aduanera.

b) Resolución Exenta N° 592 de la Dirección Nacional de Aduanas, de 13 de Febrero de 2002.

Esta disposición establece la obligación de firmar electrónicamente todas las Declaraciones de Ingreso tramitadas electrónicamente a través de las redes Públicas de Internet.

Además, indica que el despachador que utilice la Internet para su transmisión electrónica necesita la adquisición de un certificado de firma electrónica emanado de un Prestador de Servicios de Certificación de Firma Electrónica aceptado por el Servicio Nacional de Aduanas.

7.1.2.2. Normativa tributaria.

Dentro del plan de modernización del Estado, el Servicio de Impuestos Internos ha dictado normas tendientes a regular su interacción electrónica con los contribuyentes.

La seguridad electrónica se ha transformado en parte de esta relación entre el Servicio y las personas. Ello debido al crecimiento en el número de contribuyentes que realizan sus declaraciones de impuestos y trámites tributarios por Internet, lo que hace necesario el uso de una firma electrónica como reemplazante de la firma ológrafa, para quienes crean conveniente incorporar este elemento de seguridad a sus relaciones digitales con el Servicio.

⁵²⁹ Resolución Exenta N° 4.928 de la Dirección Nacional de Aduanas, de 28 de Diciembre de 2001, N° 2, IV.

La Dirección Nacional del Servicio, en virtud de las atribuciones otorgadas por el artículo 6 letra A, N° 1 del Código Tributario,⁵³⁰ ha dictado algunas resoluciones en este aspecto, siendo la más relevante la N° 9 de 15 de Febrero de 2001, publicada en el Diario Oficial el 21 de Febrero de 2001.

- **Resolución Exenta N° 9 del Servicio de Impuestos Internos, de 15 de Febrero de 2001.**

Esta resolución regula el uso de la *firma electrónica en materia tributaria*, permitiendo realizar diversos trámites, declaraciones de impuestos y declaraciones juradas a través de la transmisión electrónica vía Internet.

Así, fija las *exigencias para los contribuyentes* que decidan incorporarse al sistema de firma electrónica para acreditar su identidad digital. También establece las normas para las empresas que prestan *servicios de certificación*, “para respaldar la validez de la firma electrónica aplicada en los documentos tributarios”.⁵³¹

Además, autoriza expresamente la utilización de *certificados digitales para uso tributario*, como una forma de identificación y autenticación de los contribuyentes.

En la misma norma se señala que el Servicio *acreditará*, previamente, a las Empresas Prestadoras de Servicios de Certificación, las que, cumpliendo determinados requisitos indicados en la misma resolución, respaldarán la identidad de los contribuyentes y garantizarán la seguridad, técnica y jurídica, de las transferencias de documentos, emitiendo certificados digitales de carácter tributario.

7.2. Derecho Comparado.

Con el objeto de conocer la forma en que los diversos estados regulan la seguridad, se hará una breve referencia a las principales leyes sobre firma electrónica existentes en el mundo.

⁵³⁰ El actual Código Tributario chileno está contenido en el DL N° 830 de 1974.

⁵³¹ Magliona Markovieth, Claudio Paul, “Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico”, op. cit., apartado 3. letra c.2).

7.2.1. Ley de Utah de 1995.⁵³²

Como se indicó, ésta se constituye en la primera ley sobre firma electrónica del planeta. Ha sido fuente de inspiración para la mayoría de las leyes estatales norteamericanas y para las de otros estados.

Su importancia radica, principalmente, en que por primera vez se reconocen consecuencias jurídicas a la *firma digital*, equiparándose a la firma manuscrita.

La Ley regula la firma electrónica en base a los sistemas de *doble llave o asimétricos*. De esta forma pretende dar protección, verificación y autenticación a las transacciones electrónicas.⁵³³

Además, establece la intervención de una tercera parte confiable, las *autoridades certificadoras*, las que emiten los certificados que requiere el sistema para funcionar. Éstas necesitan, para operar, de una *licencia o autorización* del Departamento de Comercio de Utah.⁵³⁴

7.2.2. Ley alemana.

Se trata de la nueva Ley alemana sobre condiciones generales para la firma electrónica (*Gesetz über Rahmenbedingungen für elektronische Signaturen*) vigente a partir del 22 de Mayo de 2001, también llamada *Signaturgesetz* (SigG), y que sustituye a la Ley sobre Firma Electrónica de 1997 (*Gesetz zur Digitalen Signatur*).⁵³⁵

Esta norma tiene como objetivo fundamental la adecuación de la norma germana a la Directiva Europea 1999/93, pues la regulación sobre el tema, especialmente en su aspecto técnico, se encontraba desarrollada en la anterior Ley de 1997, en la Ordenanza sobre Firma Electrónica y en las publicadas “Medidas de Seguridad para las Autoridades de Certificación según la Ley sobre Firma Digital”.

⁵³² La Ley de firma electrónica del estado de Utah comenzó a regir el 1 de Mayo de 1995.

⁵³³ Devoto, Mauricio y Lynch, Horacio M, “Banca, comercio, moneda electrónica y la firma digital”, op. cit., apartado 5.

⁵³⁴ S.E. el Presidente de la República, *Proyecto de Ley sobre Firma Electrónica y los Servicios de Certificación de Firma Electrónica*, op. cit., pág. 6.

⁵³⁵ Ésta última formaba parte, como Capítulo III, del Informations-und Kommunikationsdienste-Gesetz (IuKDG) de 22 de Julio de 1997. Fernández Fernández, María Cristina, “La firma electrónica avanzada en el Derecho Europeo”, Sitio Web Universidad de Lleida, España (<http://www.udl.es>), <http://www.udl.es/dept/dpriv/law/cfernandez.doc> , pág. 5.

La vigente disposición distingue, según el grado de confianza que otorgan, entre *firma electrónica simple, avanzada y cualificada*. La primera, puede ser una imagen escaneada de una firma manuscrita, lo que aporta escasa seguridad. La firma avanzada asegura la integridad, y bajo ciertas circunstancias, la autoría. La cualificada, también otorga gran seguridad en la determinación del autor de la declaración firmada, recurriendo a las certificaciones.⁵³⁶

Respecto a los *proveedores de servicios de certificación* (llamados autoridades certificadoras según la antigua Ley) *no se establece como obligatoria la licencia* ante autoridad competente para otorgar validez a los servicios de firma electrónica. Sin embargo, los certificadores (tanto los licenciados como los no licenciados) deben cumplir, en todo caso, con los preceptos contenidos en la Ley.⁵³⁷

La nueva norma establece un sistema accesorio, mediante el cual los proveedores de servicios de certificación pueden *solicitar de forma voluntaria una acreditación a la autoridad competente*, la que garantiza la calidad y seguridad de los servicios prestados por dicho proveedor. Ello toma importancia para la firma electrónica avanzada y para la cualificada.⁵³⁸

En consecuencia, la firma electrónica que cumple con los requisitos establecidos en la Ley tiene plena validez jurídica, esté el proveedor que certifica dicha firma acreditado o no.⁵³⁹

Otro punto importante de considerar en la Ley alemana de 2001, es que no menciona las *funciones y/o efectos del uso de la firma electrónica*. Esto debido a que su objeto principal son los proveedores de servicios de certificación. El legislador alemán asume que la *Directiva Europea* establece claramente las funciones y alcance del uso de la firma electrónica. Además, las propias leyes sustantivas (el Código Civil alemán por

⁵³⁶ Fajardo López, Luis, “La Firma Electrónica en el Derecho Privado”, España, Sitio Web Luis Fajardo López (<http://www.fajardolopez.com>), http://www.fajardolopez.com/materiales/Fajardo_RJUAM.html , apartado III, letra B (“La forma del contrato”), 1 (“En otros países comunitarios. Especial referencia a Alemania”).

⁵³⁷ El sistema antiguo dejaba fuera de la regulación aquellos casos en los que no se había obtenido previamente una licencia expedida por la autoridad competente. Es más, ni siquiera podían operar como autoridad certificadora según el artículo 4. Ley alemana de 1997, Fons Lete, Emmanuel, “Comentario sobre la Directiva Europea de Firma Electrónica y la Nueva Ley Alemana de Firma Electrónica”, España, Junio de 2001. Sitio Web Foro Legal (<http://www.foro-legal.com>), http://www.foro-legal.com/publicacion_7.pdf , pág. 5.

⁵³⁸ Fons Lete, Emmanuel, “Comentario sobre la Directiva Europea de Firma Electrónica y la Nueva Ley Alemana de Firma Electrónica”, op. cit., pág. 5.

⁵³⁹ Esta limitación contradice los considerandos 12, 20 y 21 de la Directiva Europea 93/1999.

ejemplo) y procesales se preparan para recibir reformas que permitan, o excluyan en su caso, el uso de los nuevos soportes.⁵⁴⁰

7.3. Regulación internacional.

Diversas instituciones a nivel mundial intentan dar un marco de uniformidad a las diversas regulaciones estatales en materia electrónica.

El tema de la seguridad no queda al margen, por lo que la ONU y el Parlamento Europeo han elaborado documentos que se refieren a la firma electrónica, a las autoridades de certificación y a los certificados desde distintos puntos de vista.

7.3.1. Ley Modelo sobre Comercio Electrónico de UNCITRAL.⁵⁴¹

La Ley Modelo de UNCITRAL de 1996 analiza el tema de las firmas y documentos electrónicos, sin referirse específicamente a las firmas digitales o a la criptografía, manteniendo, a un nivel marco, un criterio de neutralidad tecnológica.⁵⁴² Se trata del artículo 7 de la Ley, en el cual se establece que tratándose de los mensajes de datos, la firma puede sustituirse por *un método* (cualquiera que sea) seguro de identificación del emisor.⁵⁴³

⁵⁴⁰ Fons Lete, Emmanuel, “Comentario sobre la Directiva Europea de Firma Electrónica y la Nueva Ley Alemana de Firma Electrónica”, op. cit., pág. 6.

⁵⁴¹ Elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) y aprobada por la Asamblea General de la ONU, mediante Resolución 51/162 de 1996.

⁵⁴² Jijena Leiva, Renato Javier, “Comercio, derecho, firma y documentos digitales o electrónicos”, *Análisis del Boletín N° 2348-07, sobre “Los Documentos Electrónicos”*, op. cit., pág. 47.

⁵⁴³ Zambrano Cadena, Luis Guillermo, *La Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*, op. cit., pág. 51.

7.3.2. Directiva Europea 93/1999 sobre firma digital.⁵⁴⁴

La Directiva 93/1999 fija el marco europeo para la firma electrónica, especialmente en lo que se refiere a su finalidad y alcance, así como también a los aspectos que deben ser desarrollados por cada uno de los estados miembros de la unión.⁵⁴⁵

Opta por una *neutralidad tecnológica*, por lo que no se inclina por algún sistema tecnológico de firma digital, como por ejemplo podría ser la criptografía de llave pública.⁵⁴⁶

Dos son los temas más importantes tratados por la Directiva: la definición y el reconocimiento jurídico de la firma electrónica, y la delimitación de quienes pueden ser Entidades Certificadoras.

El artículo 2º define “*firma electrónica*” como los datos en forma electrónica anexos o asociados de manera lógica a otros datos electrónicos, utilizados como medio de autenticación. Luego agrega que, de cumplir con los cuatro requisitos indicados en el N° 2 del mismo artículo, se trata de una *firma electrónica avanzada*.⁵⁴⁷

Esta última otorga mayor fiabilidad en la identificación y mayor seguridad al documento electrónico, por lo que la Directiva la equipara a la firma manuscrita, dotándola incluso de validez como prueba en juicio.⁵⁴⁸ Sin embargo, conviene precisar que la firma electrónica (a secas) también es admisible en juicio y no puede ser rechazada de plano.⁵⁴⁹ Esta regulación sobre los *efectos legales de la firma electrónica*, debe entenderse sin perjuicio de los requisitos de forma establecidos por las leyes nacionales en materia de celebración de contratos, ni de las normas que establecen el lugar en que éstos se entienden celebrados.⁵⁵⁰

⁵⁴⁴ Adoptada por el Parlamento Europeo y por el Consejo de la Unión Europea el 13 de Diciembre de 1999.

⁵⁴⁵ Fons Lete, Emmanuel, “Comentario sobre la Directiva Europea de Firma Electrónica y la Nueva Ley Alemana de Firma Electrónica”, op. cit., pág. 2.

⁵⁴⁶ Así, el Considerando Octavo establece que los rápidos avances tecnológicos y la dimensión mundial de Internet definen un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos.

⁵⁴⁷ Según la Directiva Europea 93/1999, para que exista firma electrónica avanzada, la firma debe, copulativamente: a) estar vinculada al signatario de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; d) estar vinculada a los datos a que se refiere de manera que cualquier cambio posterior de los mismos sea detectable.

⁵⁴⁸ Directiva Europea 93/1999, artículo 5 apartado primero.

⁵⁴⁹ El artículo 5 apartado segundo señala que no se negará eficacia jurídica ni se rechazará como prueba a la firma electrónica por el hecho de que se presente en forma electrónica, o no se base en un certificado reconocido, o no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o no esté creada por un dispositivo seguro de creación de firma.

⁵⁵⁰ Directiva Europea 93/1999, Considerando Diecisiete.

Respecto a los *Proveedores de Servicios de Certificación de firma electrónica* la Directiva sólo analiza requisitos esenciales mínimos, particularmente relativos a su responsabilidad frente a terceros que utilicen sus servicios. Así, el artículo 6 indica que los certificadores serán responsables por el daño ocasionado a cualquier persona que confíe en el certificado, respecto a la veracidad de la información contenida en el certificado, a la existencia de mecanismos de creación y verificación de firma, al hecho que se puedan establecer limitaciones al uso de los certificados, etc.⁵⁵¹ Esta responsabilidad se encuentra subjetivizada, ya que el certificador puede eximirse de responsabilidad si prueba que no ha actuado con negligencia.

Por último, a propósito de la *acreditación de los entes certificantes*, la Directiva opta por un sistema voluntario, “el cual se basa en condiciones objetivas, transparentes, proporcionadas y no discriminatorias (,) y cuyo objetivo es proveer un grado de confianza y seguridad superior”.^{552 553}

⁵⁵¹ Jijena Leiva, Renato Javier, “Comercio, derecho, firma y documentos digitales o electrónicos”, *Análisis del Boletín N° 2348-07, sobre “Los Documentos Electrónicos”*, op. cit., pág. 49.

⁵⁵² Directiva Europea 93/1999, artículo 3, apartados primero y segundo.

⁵⁵³ S.E. el Presidente de la República, *Proyecto de Ley sobre Firma Electrónica y los Servicios de Certificación de Firma Electrónica*, op. cit., pág. 7.

CONCLUSIONES.

El Comercio Electrónico realizado mediante la Internet ha experimentado un gran crecimiento en los últimos años. Sin embargo, éste podría incrementarse aún más, si aumentara la confianza de sus participantes, lo que se logra con un marco regulatorio que consagre y reconozca sus diversos conceptos y problemáticas. De esta forma, los posibles conflictos derivados de transacciones efectuadas a través de la Red no quedarían entregados sólo a la solución jurisprudencial.

Tres son los tópicos fundamentales que conforman el sistema del Comercio Electrónico. Se trata de los contratos electrónicos, del documento electrónico y de la seguridad. Éstos vienen a introducir nuevas instituciones al derecho y a modificar otras de carácter tradicional.

- Los *Contratos Electrónicos*, que integran este sistema debido a que el comercio en general opera a través de contratos, presentan algunas diferencias que los alejan, en alguna medida, del derecho civil clásico.

Así ocurre con el *consentimiento*, el que se produce por el concurso de la oferta y la aceptación. En este caso, ambas se realizan por medios electrónicos, lo que genera algunas dificultades en relación al momento y al lugar en que se forma el consentimiento. Es necesaria una modificación legal que regule este tema, y determine, claramente, dicho momento y lugar, ya que en este caso, resulta poco apropiado aplicar la respuesta dada por el Código de Comercio. Quizás, lo más adecuado, sería adoptar el sistema que lo considera formado una vez que el oferente recibe y tiene a su disposición el mensaje que contiene la aceptación, esto es, al igual que en la Ley Modelo de UNCITRAL sobre Comercio Electrónico, donde el receptor tenga el asiento principal de sus negocios.

Los *vicios del consentimiento* también adquieren ciertos matices en los contratos electrónicos. Esto se debe a que la voluntad se dirige a elementos que en la contratación clásica no plantearían inconveniente alguno. Además, el diálogo entre las partes es mucho menor, e incluso en ocasiones estandarizado, por lo que los vicios pueden aparecer con mayor frecuencia.

Las *formalidades* del derecho civil tienen plena aplicación en la contratación digital. Sin embargo, pueden ocasionar inconvenientes que la legislación tradicional no

previene. Si bien la Ley 19.799 intenta soslayar estos problemas, prohibiendo, en alguna medida, determinados actos solemnes (a los que se exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico), se hace necesario regular con mayor detalle este punto. Así, por ejemplo, una reforma en materia notarial y registral, permitiría la celebración de actos imposibles de celebrar en la actualidad.

Al tratar los contratos perfeccionados por medios electrónicos, se distinguieron sus tres *fases*, las que coinciden con las etapas del contrato ordinario. Sin embargo, éstas presentan algunas particularidades, especialmente, la de consumación, en la que adquieren relevancia el desarrollo de las nuevas formas de cumplir las obligaciones, como el pago electrónico, que se verifica mediante las Transferencias Electrónicas de Fondos, las que pueden adoptar diversas modalidades, siendo la más utilizada el pago con tarjeta de crédito.

Las normas relativas a la *interpretación* de los contratos establecidas por el legislador clásico, son en su mayoría aplicables a los contratos perfeccionados digitalmente. Éstos son verdaderas fuentes de interpretación de los mismos, ya que normalmente, los mensajes que contienen la oferta electrónica son profusos e incluyen las diversas posibilidades de conflicto que pueden generarse.

Por último, los *riesgos* en los contratos electrónicos no se refieren a la cosa objeto del contrato, ya que ésta continuará regida por las disposiciones establecidas en el Código Civil. Se trata de los riesgos que se generan como consecuencia de la interacción en un medio electrónico, el que puede atentar en contra de la seguridad misma del contrato y de sus cláusulas.

Todos estos matices indican que el legislador chileno debe pronunciarse en forma pormenorizada sobre los contratos electrónicos, siendo insuficiente el tratamiento dado a éstos en la Ley 19.799 (artículo 3º), la que se limita simplemente a reconocerlos. Dejar esto entregado a la jurisprudencia, no colabora con la transparencia regulatoria que requieren los usuarios del comercio electrónico.

Además de estas particularidades, los contratos electrónicos pueden dar origen a algunos *conflictos de derecho internacional privado*, ya que muchas veces involucran a agentes de procedencia diversa. La solución a éstos resulta de la adopción de un tratado internacional en el que se estipule un principio general, ello sin perjuicio de que las partes puedan someterse expresa y voluntariamente a algún ordenamiento legal

determinado. Incluso, pueden utilizarse los tratados vigentes en la actualidad, evitándose así una discriminación entre los distintos medios usados para contratar.

- Los contratos electrónicos, esto es, aquellos mediante los cuales se materializan las operaciones de comercio electrónico dan origen al *Documento Jurídico Electrónico*.

Éste tiene un carácter documental, por lo que reúne los requisitos del documento en general, pero con ciertos matices en su aspecto material, que lo diferencian del tradicional soportado en papel.

La Ley 19.799 los reconoce para el ámbito de los particulares. Sin embargo, de los órganos del Estado también pueden emanar documentos electrónicos. Para ello es necesario el reconocimiento legal de esta posibilidad, así como también el fortalecimiento de la seguridad desde un punto de vista técnico y jurídico, lo que se cumple a través del Título II de la Ley 19.799 y de su Reglamento.

Un documento digital puede ser calificado de *público*, siempre que cumpla con los requisitos que la legislación establece para tales documentos. En el caso chileno, éste debe ser autorizado por un empleado público competente con las formalidades establecidas por la ley. La intervención del funcionario competente es perfectamente posible de realizar por medios electrónicos. Sin embargo, la obligación de cumplir con las solemnidades legales sólo puede cumplirse con una legislación que adapte éstas, en cada caso, a estos nuevos documentos.

Los documentos electrónicos se admiten espontáneamente *como medio de prueba* en los sistemas de libre apreciación. En los de prueba tasada sólo es posible su incorporación al sistema probatorio mediante la dictación de una norma que los establezca expresamente. En Chile, se les reconoce mérito probatorio a través de diversas disposiciones legales, siendo la más importante la Ley 19.799.

Las legislaciones de un gran número de países en el mundo otorgan validez jurídica y valor probatorio al documento electrónico. Sin embargo, ello aún no es suficiente ni tiene la velocidad con la que se desarrolla el comercio electrónico en la práctica.

- La Internet es el medio a través del cual se efectúan la mayoría de las transacciones comerciales electrónicas. Ésta es una red abierta, a la que tienen acceso las personas sin restricción alguna, por lo que los contratos, documentos y en general

cualquier operación que la utilice, debe contar con determinadas medidas de seguridad que protejan la información.

Se trata de cumplir con ciertos *principios indispensables*, necesarios para que los mensajes electrónicos sean considerados seguros, como son: la confidencialidad, la integridad, la autenticación y el no repudio.

Actualmente, la solución tecnológica utilizada para dar cumplimiento a estos requerimientos jurídicos se basa en los *sistemas criptográficos*, principalmente en los asimétricos. Estos mecanismos, a través de la firma electrónica y los certificados otorgados por entidades certificadoras, conforman la estructura de seguridad de los mensajes electrónicos, y en consecuencia, resultan esenciales para el desarrollo de un comercio electrónico seguro.

Los sistemas criptográficos en general permiten resolver los problemas de seguridad relativos a la integridad y a la confidencialidad de los mensajes, más no así los de certeza sobre la autenticidad y el no rechazo, los que requieren específicamente de las firmas digitales, las que constituyen mecanismos de encriptación más elaborados.

Respecto a éstas, hoy la más utilizada es la *firma electrónica* con encriptación asimétrica o de doble clave. Sin embargo, con el fin de evitar la obsolescencia a corto plazo, las diversas legislaciones, entre ellas la chilena, tienden a adoptar el principio de neutralidad tecnológica, por lo que regulan sólo los efectos de dicha firma y no su tecnología que evoluciona todos los días.

La Ley 19.799 reconoce jurídicamente a la firma digital y le otorga los mismos efectos que a la firma manuscrita. Además establece la *firma electrónica avanzada*, la que es requerida para que un documento electrónico tenga la calidad de instrumento público, y para que hagan plena prueba, en caso de ser presentados en juicio, los documentos electrónicos que tengan la calidad de instrumento público y los que posean la calidad de instrumento privado cuando hayan sido firmados mediante firma electrónica avanzada.

Del concepto legal de firma electrónica avanzada es posible desprender que ella está muy relacionada con la certificación emanada de un prestador de servicios. Es más, la ley los regula extensamente, lo que permite concluir, que en este punto, la Ley 19.799 tiende a alejarse del principio de neutralidad tecnológica, dejándolo, como ya se indicó, sólo para la firma electrónica “a secas”.

Los *certificados digitales* tienen por objeto acreditar la identidad del emisor o receptor de un mensaje electrónico. La identificación del sujeto se produce a través del

correspondiente certificado, el cual vincula a un suscriptor con una determinada firma electrónica. La política legislativa de los estados determina si estas actividades de identificación las desarrollan entes públicos o privados.

Los certificados que funcionan sobre la base de sistemas asimétricos de encriptación se constituyen, actualmente, en un elemento de carácter sustancial para la aplicación segura de la tecnología de firma electrónica en el ámbito del comercio electrónico. Ello debido a que colaboran en la resolución del problema de la distribución fiable de llaves públicas (a través de la comprobación de la identidad del titular).

Por último, las transacciones comerciales electrónicas, para ser seguras, requieren de la intervención de una tercera parte de confianza, la que cuando realiza la función específica de emitir certificados se denomina, según la ley chilena, *Prestador de Servicios de Certificación*, o simplemente, *Certificador*.

En resumen, de los tres temas tratados en esta memoria, la Seguridad es el único que ha alcanzado un desarrollo aceptable de parte del legislador chileno (en la Ley 19.799 y en su Reglamento).

Los otros, requieren un mayor tratamiento, ya que si bien la Ley los reconoce, ello no es suficiente para responder a la serie de cuestionamientos que se derivan de su existencia. Si bien la legislación tradicional (civil, mercantil y procesal) puede ser interpretada en forma extensiva, aplicando sus normas al contrato y al documento electrónico, en caso de conflicto, no otorgan la suficiente certeza que requieren los particulares para actuar en el ámbito electrónico.

Sólo el perfeccionamiento de la legislación relativa al comercio electrónico, puede generar la confianza que requieren sus participantes, para que éste crezca y se desarrolle sin trabas.

BIBLIOGRAFÍA.

I. Libros y artículos.

Abeliuk Manasevich, René, *Las Obligaciones*, Tomos I y II, Tercera Edición, Editorial Jurídica de Chile, Santiago, Chile, 1993, pp.1.066.

Bacchetta, Marc, et al., *El comercio electrónico y el papel de la OMC*, Estudios especiales, Publicaciones de la OMC, Ginebra, Suiza, 1998, pp.83.

Candelario Macías, Isabel, “Breves apuntes sobre la normación del Comercio Electrónico”, (c 2000, IBDI). Sitio Web Instituto Brasileiro de Política e Direito da Informática (IBDI) (<http://www.ibdi.hpg.ig.com.br/artigos/>), http://www.ibdi.hpg.ig.com.br/artigos/isabel_candelario/001.html .

Canales, Patricia, “El valor probatorio de los documentos electrónicos en los países pertenecientes a la Unión Europea”, *Serie Estudios*, Año V, N° 119, Departamento de Estudios y Extensión, Biblioteca del Congreso Nacional de Chile, Santiago, Chile, Noviembre, 1995.

Carrasco Blanc, Humberto, “Comentarios relativos a las normas sobre el consentimiento y su interacción con las nuevas tecnologías de la información”, *Revista de Derecho Informático (REDI)*, N° 98, Noviembre 2001, (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/40-16.asp> .

Carrasco Blanc, Humberto, “Contratos informáticos y Ley del Consumidor Chilena”, *Revista de Derecho Informático (REDI)*, N° 15, Octubre 1999, (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/revista.asp?idRevista=17> .

Carrascosa López, Valentín, et al., *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, España, Editorial Comares S.L., 1997, pp.356.

Carvajal Sánchez, Bernardo Andrés, *Algunos aspectos jurídicos relevantes para el desarrollo del comercio electrónico. Aproximación a las necesidades jurídicas de sus agentes económicos*, Bogotá, Septiembre 2000, Tesis (Licenciatura en Derecho), Universidad Externado de Colombia. *Revista de Derecho Informático (REDI)*, N° 99, Diciembre 2001 (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/revista.asp?idRevista=42> .

Casarino Viterbo, Mario, *Manual de derecho procesal. Derecho procesal civil*, Tomo IV, Quinta Edición, Editorial Jurídica de Chile, Santiago, Chile, 2000, pp.470.

Connelly, Thomas, “Compraventa mediante Tarjeta de Crédito a través del Internet”, Serie Informes Año IX, N° 69, Departamento de Estudios, Extensión y Publicaciones, Biblioteca del Congreso Nacional de Chile, Santiago, Chile, Septiembre de 1999.

Cornejo López, Valentino, “Testigos Electrónicos ante la Dificultad de la Contratación Electrónica en el Derecho Mexicano”, *REDI: Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., N° 34, Mayo 2001(c 1997-2002, vLex Networks). Sitio Web vLex, España (http://v2.vlex.com/global/redi/redi_default.asp), http://v2.vlex.com/es/ppv/doctrina/fuente_29,numero_%2334 .

Corporación Tiempo 2 Mil, “Algunos Aspectos del Comercio Electrónico y su Regulación” (Tema de Opinión), *Bitácora Legislativa*, Programa de Asesoría Legislativa, Santiago, 15 al 19 Mayo de 2000, -19-29-.

Corporación Tiempo 2 Mil, “Proyecto de Ley que establece normas sobre documentos electrónicos” (Ficha Legislativa N° 989), *Bitácora Legislativa*, Programa de Asesoría Legislativa, Santiago, 20 al 24 de Marzo de 2000, -3-20-.

Cruz Cruz, Sergio, “Contratación electrónica: Hacia un modelo de confianza”, Sitio Web Escuela de Derecho de la Universidad Diego Portales, Chile (<http://derecho.udp.cl>), <http://derecho.udp.cl/e/materiales/internet/modelo%20confianza.PDF> .

Devoto, Mauricio y Lynch, Horacio M., “Banca, comercio, moneda electrónica y la firma digital”. *Revista de Derecho Informático (REDI)*, No.2, Septiembre 1998 (c1998-2003, Alfa Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/3-3.asp> .

Espina, Alberto y Walker Patricio, *Proyecto de Ley sobre Comunicaciones Electrónicas*, Boletín N° 2512-07, Cámara de Diputados, Valparaíso, Chile, 2000, pp. 48.

Etcheberry, Alfredo, *Derecho Penal*, Tomo IV, Parte Especial, Tercera Edición (revisada y actualizada), Editorial Jurídica de Chile Santiago, Chile, 1998.

Fajardo López, Luis, “La Firma Electrónica en el Derecho Privado”, España, Sitio Web Luis Fajardo López (<http://www.fajardolopez.com>), http://www.fajardolopez.com/materiales/Fajardo_RJUAM.html .

Fernández Acevedo, Fernando, “Responsabilidad Civil de los Prestadores de Servicios de Certificación”, *Revista de Derecho Informático (REDI)*, N° 109, Octubre 2002 (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/upload/revista/101502--19-51-publicación.doc> .

Fernández Fernández, María Cristina, “La firma electrónica avanzada en el Derecho Europeo”, Sitio Web Universidad de Lleida, España (<http://www.udl.es>), <http://www.udl.es/dept/dpriv/law/cfernandez.doc> .

Fons Lete, Emmanuel, “Comentario sobre la Directiva Europea de Firma Electrónica y la Nueva Ley Alemana de Firma Electrónica”, España, Junio de 2001.

Sitio Web Foro Legal (<http://www.foro-legal.com>), http://www.foro-legal.com/publicacion_7.pdf .

Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, Primera Edición, Barcelona, Editorial Bosch S.A., Abril 2000, pp. 525.

Gaete González, Eugenio Alberto, “Documento electrónico e instrumento público”, *Revista de Derecho Informático (REDI)*, N° 24, Julio 2000, (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/25-8.asp> .

González Cristóbal, “La firma y el documento electrónico en relación a su valor probatorio”, *Revista de Derecho Informático (REDI)* N° 101, Febrero 2002, (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi. (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/45-11.asp> .

Gutiérrez Morán, Rodrigo, et al. . “Informe Jurídico para un modelo de esquema de confianza en el Comercio Electrónico”, Santiago, 24 de Julio de 2000. Sitio Web Escuela de Derecho de la Universidad Diego Portales, Chile (<http://derecho.udp.cl/e/publicaciones.htm>), <http://derecho.udp.cl/e/publicaciones/modelo%20de%20confianza.PDF> .

Hance, Olivier y Dionne Balz, Suzan, *Leyes y Negocios en Internet*, Primera Edición, México, Mc Graw-Hill Interamericana Editores, S.A., Diciembre 1996 (c 1996), pp.371, (*Business and Law on the Internet* (c1996, Best of Publishing), tr. Yazmin Juárez Parra).

Herrera Bravo, Rodolfo, “El documento electrónico: algunas vías de aplicación en el Derecho Probatorio Chileno”, *Revista de Derecho Informático (REDI)*, N° 7, Febrero 1999, (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/8-4.asp> .

Iglesias, Marco A., “La Primera Piedra del Comercio Electrónico”, *Revista del Abogado*, Publicación del colegio de Abogados de Chile, N° 17, Santiago, Noviembre 1999, -18-19-.

Illescas, Rafael, “El Comercio Electrónico Internacional: su Gobierno”, *Revista Jurídica del Perú*, Año XLVII, N° 12, Lima, Perú, Julio-Septiembre 1997,-203-207-.

Irabien, José Fernando “Key Management y Certificación Digital”, *Revista de Derecho Informático (REDI)*, N° 110, Noviembre 2002 (c1998-2003, Alfa Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/54-5.asp> .

Jijena Leiva, Renato Javier, “Comercio, derecho, firma y documentos digitales o electrónicos”, *Análisis del Boletín N° 2348-07, sobre “Los Documentos Electrónicos”*, Informe preparado para los trabajos de la Comisión de Constitución, Legislación, Justicia y Reglamento del Honorable Senado de la República, en respuesta al Oficio L-N° 52/99, Valparaíso, Julio 1999.

Jijena Leiva, Renato Javier, “Comercio electrónico, derecho y firma digital”, *Revista Infoweek*, N° 78, 17 al 6 de Julio de 1999, -12-.

Jijena Leiva, Renato Javier, “Comercio electrónico y derecho. La problemática jurídica del Comercio Electrónico”, *REDI: Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., N° 9, Abril 1999 (c 1997-2002, vLex Networks). Sitio Web [vlex.com](http://v2.vlex.com), España
(http://v2.vlex.com/global/redi/redi_numero.asp?numero=%239&fecha=Abril+1999),
http://v2.vlex.com/es/ppv/doctrina/fuente_29,numero_%239 .

Jijena Leiva, Renato Javier, “Comercio, Firma Digital y Derecho”, *Revista del Abogado*, Publicación del Colegio de Abogados de Chile, N° 24, Abril 2002. Sitio Web Colegio de Abogados de Chile (<http://www.abogados.cl> ; Revista del Abogado; Números anteriores).

Jijena Leiva, Renato Javier, “Naturaleza jurídica y valor probatorio del documento electrónico. El caso de la declaración de importación electrónica o mensaje CUSDEC”, *Revista de Derecho de la Universidad Católica de Valparaíso*, N° XIX, Ediciones Universitarias de Valparaíso, Valparaíso, Chile, 1998,-457-475-.

Magliona Markovitch, Claudio Paul, “Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico”, *Revista de Derecho Informático (REDI)*, N° 34, Mayo 2001 (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/data/35-9.asp> .

Maldonado Sergio, “Validez transfronteriza de contratos on-line”, 2000 (c 2000, Sergio Maldonado), Sitio Web Sergio Maldonado, http://www.smaldonado.com/search/collections/english/evidence_es.htm .

Márquez González, José Antonio, “¿Cuándo se perfecciona un contrato? Sobre Contratación Electrónica, REDI: *Revista Electrónica de Derecho Informático*, Edita vLex Networks s.l., N° 36, Julio 2001 (c 1997-2002, vLex Networks). Sitio Web vlex.com, España (http://v2.vlex.com/global/redi/redi_numero.asp?numero=%239&fecha=Abril+1999), <http://v2.vlex.com/es/ppv/doctrina/fuente.asp?fuente=29&numero=%2336> .

Martínez Nadal Apol.lònia, *Comercio electrónico, firma digital y autoridades de certificación*, Primera Edición, Madrid, Editorial Civitas, 1998, pp.294.

Martino, Antonio A, “Reconocimiento del Valor Jurídico del Documento Digital en Italia: Breve Historia de una Ley”, (c 2000, Notaría Digital). Sitio Web Notaría Digital, (<http://www.notariadigital.com> ; Boletín Digital; Índice Boletín), <http://www.notariadigital.com/boletin.htm> .

Millé, Antonio, “Impacto del Comercio Electrónico sobre la Propiedad Intelectual”, Actas del II Congreso Chileno de Derecho Privado, *Revista de Derecho de la Universidad Católica de Valparaíso*, N° XIX, Ediciones Universitarias de Valparaíso, Valparaíso, Chile, 1998, -339-369-.

Ministerio de Justicia Español, “La firma y el comercio electrónico. Aspectos jurídicos de los servicios de la sociedad de la información”, Madrid, 7 de Diciembre de 1999 (c 1998-2003, Asociación de Internautas), Sitio Web Asociación de Internautas (www.internautas.org/ ; Documentos),
http://www.internautas.org/documentos/mj_firmacomer.htm#5 .

Moreno Monroy, René, *Apuntes de clases*, Derecho Civil I, Universidad de Valparaíso, 1994.

Moreno Navarrete, Miguel Ángel, “Hacia una regulación positiva del documento electrónico. El modelo italiano”, España (c 2000, Notaría Digital). Sitio Web Notaría Digital (www.notariadigital.com ; Boletín Digital; Índice Boletín),
<http://www.notariadigital.com/boletin.htm> .

Núñez Rojas, Juan, *El contrato de compraventa a través de Internet*, Chile 2000, pp. 105. Tesis (Licenciatura en Derecho), Facultad de Ciencias Jurídicas y Sociales, Escuela de Derecho Universidad Central de Chile.

Otero Alvarado, Jorge y Lanckenau, René, *Comercio Electrónico. Generalidades y Problemáticas Jurídicas*, Estudio Jurídico Otero, ENTEL Internet, Santiago, Chile, 1999, pp.71.

Paladella Salord, Carlos de, “El documento electrónico como prueba-La Reforma del Código Civil Francés”, Septiembre 2000. Sitio Web Carlos de Paladella (<http://comunidad.derecho.org/carlospaladella> ; Artículos propios),
<http://comunidad.derecho.org/carlospaladella/cps6.pdf> .

Pérez Pereira, María, “Hacia la seguridad en el Comercio Electrónico”, REDI: *Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., N° 11, Junio 1999 (c 1997-2002, vLex Networks). Sitio Web “vLex”, España (http://v2.vlex.com/global/redi/redi_default.asp),
<http://v2.vlex.com/es/ppv/doctrina/fuente.asp?fuelle=29&numero=%2311> .

Piaggi, Ana I., “El Comercio Electrónico y el Nuevo Escenario de los Negocios”, *Contribuciones*, publicación trimestral de la Fundación Konrad Adenauer- Centro Interdisciplinario de Estudios sobre el Desarrollo Latinoamericano (CIEDLA), Año XVI, Nº 4, Buenos Aires, Argentina, Octubre-Diciembre 1999, -181-191-.

Pinochet, Olave, “Algunas deficiencias de la nueva legislación sobre firma electrónica y documento electrónico”, Junio 2000. Sitio Web Noticias jurídicas (<http://noticias.juridicas.com/> ; Artículos; Informático), http://noticias.juridicas.com/areas_virtual/Articulos/20-Derecho%20Inform%20Etico/200006-fe.htm .

Prieto Sánchez, José María, “El documento electrónico en la Administración Pública”, *Boletín Jurídico Derecho.com*, Nº 9, 15 al 31 de Enero 2001 (c 1997, Derecho.com). Sitio Web Derecho.com (<http://www.derecho.com/boletinesjuridicos/>), <http://www.derecho.com/boletin/articulos/articulo0027.htm> .

Ramos Suárez, Fernando, “Problemas jurídicos del Comercio Electrónico”, *REDI: Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., Nº 2, Septiembre 1998 (c 1997-2002, vLex Networks). Sitio Web vLex, España (http://v2.vlex.com/global/redi/redi_default.asp), http://v2.vlex.com/es/ppv/doctrina/fuente_29,numero_%232 .

Real Academia Española, *Diccionario de la Lengua Española*, Decimonovena Edición, Editorial Espasa-Calpe, Madrid, 1970.

Revista Barras, “Derecho y Comercio Electrónico: el Desafío de No Quedarse Atrás”, *Barras, la Revista del Comercio Electrónico*, Nº 33, Santiago, Chile, Diciembre-Enero 1999, -24-26-.

Ribas, Xavier, “Comercio electrónico en Internet. Aspectos jurídicos”, *REDI: Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., Nº 1, Agosto 1998 (c 1997-2002, vLex Networks). Sitio Web vLex, España (http://v2.vlex.com/global/redi/redi_default.asp), http://v2.vlex.com/es/ppv/doctrina/fuente_29,numero_%231 .

Rico Carrillo, Mariliana, “El documento electrónico como medio de prueba”. Ponencia presentada en el Simposio Argentino de Informática y Derecho, 11 y 12 de Septiembre de 2001, Universidad de Buenos Aires, Argentina, <http://elciruelo.freeservers.com/Ponencia11.pdf> , versión html.

Rico Carrillo, Mariliana, “Validez y regulación legal del documento y la contratación electrónica”, *REDI: Revista Electrónica de Derecho Informático*, Edita vLex Networks S.L., N° 19, Febrero 2000(c 1997-2002, vLex Networks). Sitio Web vLex, España (http://v2.vlex.com/global/redi/redi_default.asp), http://v2.vlex.com/es/ppv/doctrina/fuente_29,numero_%2319 .

Ruiz, Fernando, “El documento electrónico frente al derecho civil y financiero”, *Revista de Derecho Informático (REDI)*, N° 16, Noviembre 1999 (c1998-2003, Alfa-Redi). Sitio Web Comunidad Alfa-Redi (<http://www.alfa-redi.org/> ; Histórico), <http://www.alfa-redi.org/revista/revista.asp?idRevista=16#> .

S.E. el Presidente de la República, *Proyecto de Ley sobre Firma Electrónica y los Servicios de Certificación de Firma Electrónica*, Cámara de Diputados (Boletín 2571-19), Valparaíso, 22 de Agosto de 2000, pp.46.

Servidio de Mastronardi, Ana María, “Consideraciones acerca del Documento Electrónico y la Seguridad Jurídica”, *Revista de la Universidad Blas Pascal*, Córdoba, Argentina, N° 4, 1993 (c 1993, Universidad Blas Pascal). Sitio Web Universidad Blas Pascal, Argentina (<http://www.ubp.edu.ar/investigacion/revistas/>), <http://www.ubp.edu.ar/investigacion/revistas/revista4/art6.html> .

Vinje, Thomas C., “La Directiva de la Unión Europea en materia de Comercio Electrónico”, *Revista Derecho y Nuevas Tecnologías*, N° 3, Año 2, Editorial AD. HOC, Buenos Aires, Argentina, 2000,-87-94-.

Vodanovich H., Antonio, *Curso de Derecho Civil, Parte General y los Sujetos de Derecho*, explicaciones basadas en las clases de los profesores de la Universidad de

Chile, Arturo Alessandri Rodríguez y Manuel Somarriva Undurraga, Cuarta Edición, Editorial Nascimento, Santiago, Chile, 1971, pp.591.

Zambrano Cadena, Luis Guillermo, *La Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*. Chile, 1997, pp.96. Tesis (Licenciatura en Derecho), Universidad de Concepción, Facultad de Ciencias Jurídicas y Sociales.

II. Normas nacionales.

Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, publicada en el Diario Oficial el 12 de abril del año 2002.

Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, Decreto Supremo N° 181 del Ministerio de Economía, Fomento y Reconstrucción de 9 de Julio de 2002, publicado en el Diario Oficial el 17 de Agosto de 2002.

Ley 19.496 que establece normas sobre protección de los derechos de los consumidores, publicada en el Diario Oficial el 7 de marzo de 1997.

Código Civil de la República de Chile, aprobado el 14 de Diciembre de 1855.

Código de Comercio de la República de Chile, aprobado el 23 de Noviembre de 1865.

Manual de Procedimientos Operativos para la Transmisión Electrónica de Documentos y sus Anexos, correspondiente a la Resolución del Director Nacional de Aduanas N° 1681 de 8 de Abril de 1999, modificada por la Resolución N° 1670 de 3 de Mayo de 2001(que reemplaza los Capítulos I al V e incorpora los Anexos N° 8 al 12) y por la Resolución Exenta N° 4928 de 28 de Diciembre de 2001(que modifica el Subcapítulo III del Capítulo III).

Resolución Exenta N° 592 de la Dirección Nacional de Aduanas, de 13 de Febrero de 2002.

Resolución Exenta N° 9 del Servicio de Impuestos Internos, de 15 de Febrero de 2001.

III. Normas extranjeras.

Alemania, Ley sobre condiciones generales para la firma electrónica (*Gesetz über Rahmenbedingungen für elektronische Signaturen*), vigente a partir del 22 de Mayo de 2001.

España, Ley de Enjuiciamiento Civil, 7 de Enero del año 2000.

España, Real Decreto-Ley sobre firma electrónica, 17 de Septiembre de 1999.

Estados Unidos, Ley de firma Digital del estado de Utah, (*Digital Signature Act*), 1 de mayo de 1995.

Francia, Ley N° 2000-230, sobre adaptación del derecho de prueba a las nuevas tecnologías de la información y relativa a la firma electrónica, 13 de marzo de 2000.

Italia, Reglamento de actos, documentos y contratos en forma electrónica, Decreto N° 513 de 10 de Noviembre de 1997.

IV. Tratados y Convenios Internacionales.

Ley Modelo sobre Comercio Electrónico, UNCITRAL (Comisión de Naciones Unidas para el Derecho Mercantil Internacional), aprobada en su vigésimo noveno período de sesiones, correspondiente al quincuagésimo primer período de sesiones de la Asamblea General de Naciones Unidas, 12 de Junio de 1996.

Convención de la Haya sobre Ley aplicable a las compraventas con carácter internacional de bienes muebles corporales, 15 de Junio de 1955. Entrada en vigencia: 1 de septiembre de 1964.

Convenio Europeo sobre Ley aplicable a las obligaciones contractuales, Roma, 19 de Junio de 1980. Entrada en vigencia: 1 de Abril de 1991.

Convención de Viena sobre la Compraventa Internacional de Mercaderías, Naciones Unidas, 11 de Abril de 1980. Entrada en vigencia: 1 de Enero de 1988.

“Recomendación en el valor legal de los registros de computadora (*Legal Value of Computer Records*), UNCITRAL, décimo octava sesión, 1985.

Directiva Europea 93/1999 sobre firma digital, del Parlamento Europeo y del Consejo de la Unión Europea, de 13 de Diciembre de 1999.

Directiva Europea 31/2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico (Directiva sobre el Comercio Electrónico), del Parlamento Europeo y del Consejo de la Unión Europea, de 8 de Junio de 2000.

ANEXO.

I. LEY 19.799 SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y SERVICIOS DE CERTIFICACION DE DICHA FIRMA.⁵⁵⁴

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente Proyecto de ley:

"LEY SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y SERVICIOS DE CERTIFICACION DE DICHA FIRMA

TITULO I

Disposiciones Generales

Artículo 1º.- La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso.

Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel.

Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados.

Artículo 2º.- Para los efectos de esta ley se entenderá por:

- a) Electrónico: característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;
- b) Certificado de firma electrónica: certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica;
- c) Certificador o Prestador de Servicios de Certificación: entidad prestadora de servicios de certificación de firmas electrónicas;
- d) Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior;
- e) Entidad Acreditadora: la Subsecretaría de Economía, Fomento y Reconstrucción;
- f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor;
- g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere,

⁵⁵⁴ Publicada en el Diario Oficial el día 12 abril 2002.

permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría, y

h) Usuario o titular: persona que utiliza bajo su exclusivo control un certificado de firma electrónica.

Artículo 3º.- Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.

Lo dispuesto en el inciso anterior no será aplicable a los actos o contratos otorgados o celebrados en los casos siguientes:

a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico;

b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes, y

c) Aquellos relativos al derecho de familia.

La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en los artículos siguientes.

Artículo 4º.- Los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada.

Artículo 5º.- Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes:

1.- Los señalados en el artículo anterior, harán plena prueba de acuerdo con las reglas generales, y

2.- Los que posean la calidad de instrumento privado tendrán el mismo valor probatorio señalado en el número anterior, en cuanto hayan sido suscritos mediante firma electrónica avanzada. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales.

TITULO II

Uso de Firmas Electrónicas por los Órganos del Estado

Artículo 6º.- Los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica.

Se exceptúan aquellas actuaciones para las cuales la Constitución Política o la ley exija una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas.

Lo dispuesto en este Título no se aplicará a las empresas públicas creadas por ley, las que se regirán por las normas previstas para la emisión de documentos y firmas electrónicas por particulares.

Artículo 7º.- Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel.

Con todo, para que tengan la calidad de instrumento público o surtan los efectos propios de éste, deberán suscribirse mediante firma electrónica avanzada.

Artículo 8°.- Las personas podrán relacionarse con los órganos del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito por la ley y que tales técnicas y medios sean compatibles con los que utilicen dichos órganos.

Los órganos del Estado deberán evitar, al hacer uso de firmas electrónicas, que se restrinja injustificadamente el acceso a las prestaciones que brinden y a la publicidad y transparencia que rijan sus actuaciones y, en general, que se cause discriminaciones arbitrarias.

Artículo 9°.- La certificación de las firmas electrónicas avanzadas de las autoridades o funcionarios de los órganos del Estado se realizará por los respectivos ministros de fe. Si éste no se encontrare establecido en la ley, el reglamento a que se refiere el artículo 10 indicará la forma en que se designará un funcionario para estos efectos.

Dicha certificación deberá contener, además de las menciones que corresponda, la fecha y hora de la emisión del documento.

Los efectos probatorios de la certificación practicada por el ministro de fe competente serán equivalentes a los de la certificación realizada por un prestador acreditado de servicios de certificación.

Sin perjuicio de lo dispuesto en el inciso primero, los órganos del Estado podrán contratar los servicios de certificación de firmas electrónicas con entidades certificadoras acreditadas, si ello resultare más conveniente, técnica o económicamente, en las condiciones que señale el respectivo reglamento.

Artículo 10.- Los reglamentos aplicables a los correspondientes órganos del Estado regularán la forma cómo se garantizará la publicidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, y las demás necesarias para la aplicación de las normas de este Título.

TITULO III

De los Prestadores de Servicios de Certificación

Artículo 11.- Son prestadores de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Asimismo, son prestadores acreditados de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en Chile y acreditadas en conformidad al Título V de esta ley, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Artículo 12.- Son obligaciones del prestador de servicios de certificación de firma electrónica:

a) Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano;

b) Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el

reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley N° 19.628, sobre Protección de la Vida Privada;

c) En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad;

d) Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten;

e) En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;

f) Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores;

g) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que dará a los datos de los certificados, especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;

h) En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere;

i) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos, y

j) Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes N° 19.496, sobre Protección de los Derechos de los Consumidores, y N° 19.628, sobre Protección de la Vida Privada.

Artículo 13.- El cumplimiento por parte de los prestadores no acreditados de servicios de certificación de firma electrónica, de las obligaciones señaladas en las letras a), b), c) y j) del artículo anterior, será considerado por el juez como un antecedente para determinar si existió la debida diligencia, para los efectos previstos en el inciso primero del artículo siguiente.

Artículo 14.- Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación

u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.

Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica.

Para los efectos de este artículo, los prestadores acreditados de servicios de certificación de firma electrónica deberán contratar y mantener un seguro, que cubra su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por aquellos homologados en virtud de lo dispuesto en el inciso final del artículo 15.

El certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero. El proveedor de servicios de certificación quedará eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado.

En ningún caso la responsabilidad que pueda emanar de una certificación efectuada por un prestador privado acreditado comprometerá la responsabilidad pecuniaria del Estado.

TITULO IV

De los Certificados de Firma Electrónica

Artículo 15.- Los certificados de firma electrónica, deberán contener, al menos, las siguientes menciones:

- a) Un código de identificación único del certificado;
- b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada;
- c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y
- d) Su plazo de vigencia.

Los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en esta ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente.

Artículo 16.- Los certificados de firma electrónica quedarán sin efecto, en los siguientes casos:

- 1) Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión;
- 2) Por revocación del prestador, la que tendrá lugar en las siguientes circunstancias:
 - a) A solicitud del titular del certificado;
 - b) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso;
 - c) Por resolución judicial ejecutoriada, o
 - d) Por incumplimiento de las obligaciones del usuario establecidas en el artículo 24;
- 3) Por cancelación de la acreditación y de la inscripción del prestador en el registro de prestadores acreditados que señala el artículo 18, en razón de lo dispuesto en el artículo 19 o del cese de la actividad del prestador, a menos que se verifique el traspaso

de los datos de los certificados a otro prestador, en conformidad con lo dispuesto en las letras c) y h) del artículo 12, y

4) Por cese voluntario de la actividad del prestador no acreditado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad a la letra c) del artículo 12.

La revocación de un certificado en las circunstancias de la letra d) del número 2) de este artículo, así como la suspensión cuando ocurriere por causas técnicas, será comunicada previamente por el prestador al titular del certificado, indicando la causa y el momento en que se hará efectiva la revocación o la suspensión. En cualquier caso, ni la revocación ni la suspensión privarán de valor a los certificados antes del momento exacto en que sean verificadas por el prestador.

El término de vigencia de un certificado de firma electrónica por alguna de las causales señaladas precedentemente será inoponible a terceros mientras no sea eliminado del registro de acceso público.

TITULO V

De la Acreditación e Inspección de los Prestadores de Servicios de Certificación

Artículo 17.- La acreditación es el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Entidad Acreditadora que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en esta ley y en el reglamento, permitiendo su inscripción en el registro que se señala en el artículo 18.

Para ser acreditado, el prestador de servicios de certificación deberá cumplir, al menos, con las siguientes condiciones:

- a) Demostrar la fiabilidad necesaria de sus servicios;
- b) Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos;
- c) Emplear personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados;
- d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;
- e) Haber contratado un seguro apropiado en los términos que señala el artículo 14, y
- f) Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación.

Artículo 18.- El procedimiento de acreditación se iniciará mediante solicitud ante la Entidad Acreditadora, a la que se deberá acompañar los antecedentes relativos a los requisitos del artículo 17 que señale el reglamento y el comprobante de pago de los costos de la acreditación. La Entidad Acreditadora deberá resolver fundadamente sobre la solicitud en el plazo de veinte días contados desde que, a petición del interesado, se certifique que la solicitud se encuentra en estado de resolverse. Si el interesado enunciare el incumplimiento de ese plazo ante la propia autoridad y ésta no se pronunciare dentro del mes siguiente, la solicitud se entenderá aceptada.

La Entidad Acreditadora podrá contratar expertos con el fin de verificar el cumplimiento de los requisitos señalados en el artículo 17.

Otorgada la acreditación, el prestador será inscrito en un registro público que a tal efecto llevará la Entidad Acreditadora. Durante la vigencia de su inscripción en el

registro, el prestador acreditado deberá informar a la Entidad Acreditadora cualquier modificación de las condiciones que permitieron su acreditación.

Artículo 19.- Mediante resolución fundada de la Entidad Acreditadora se podrá dejar sin efecto la acreditación y cancelar la inscripción en el registro señalado en el artículo 18 por alguna de las siguientes causas:

- a) Solicitud del prestador acreditado;
- b) Pérdida de las condiciones que sirvieron de fundamento a su acreditación, la que será calificada por los funcionarios o peritos que la Entidad Acreditadora ocupe en la inspección a que se refiere el artículo 20, y
- c) Incumplimiento grave o reiterado de las obligaciones que establece esta ley y su reglamento.

En los casos de las letras b) y c), la resolución será adoptada previa audiencia del afectado y se podrá reclamar de ella ante el Ministro de Economía, Fomento y Reconstrucción, dentro del plazo de cinco días contados desde su notificación. El Ministro tendrá un plazo de treinta días para resolver. Dentro de los diez días siguientes a la fecha en que se notifique la resolución que éste dicte o, en su caso, desde que se certifique que la reclamación administrativa no fue resuelta dentro de plazo, el interesado podrá interponer reclamación jurisdiccional, para ante la Corte de Apelaciones de su domicilio. La reclamación deberá ser fundada y para su agregación a la tabla, vista y fallo, se regirá por las normas aplicables al recurso de protección. La resolución de la Corte de Apelaciones no será susceptible de recurso alguno.

Los certificadores cuya inscripción haya sido cancelada, deberán comunicar inmediatamente este hecho a los titulares de firmas electrónicas certificadas por ellos. Sin perjuicio de ello, la Entidad Acreditadora publicará un aviso dando cuenta de la cancelación, a costa del certificador. A partir de la fecha de esta publicación, quedarán sin efecto los certificados, a menos que los datos de los titulares sean transferidos a otro certificador acreditado, en conformidad con lo dispuesto en la letra h) del artículo 12. Los perjuicios que pueda causar la cancelación de la inscripción del certificador para los titulares de los certificados que se encontraban vigentes hasta la cancelación, serán de responsabilidad del prestador.

Artículo 20.- Con el fin de comprobar el cumplimiento de las obligaciones de los prestadores acreditados, la Entidad Acreditadora ejercerá la facultad inspectora sobre los mismos y podrá, a tal efecto, requerir información y ordenar visitas a sus instalaciones mediante funcionarios o peritos especialmente contratados, de conformidad al reglamento.

Artículo 21.- La Entidad Acreditadora, así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen los certificadores acreditados.

Artículo 22.- Los recursos que perciba la Entidad Acreditadora por parte de los prestadores acreditados de servicios de certificación constituirán ingresos propios de dicha entidad y se incorporarán a su presupuesto.

TITULO VI

Derechos y Obligaciones de los Usuarios de Firmas Electrónicas

Artículo 23.- Los usuarios o titulares de firmas electrónicas tendrán los siguientes derechos:

1°. A ser informado por el prestador de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, previamente a que se empiece a efectuar;

2°. A la confidencialidad en la información proporcionada a los prestadores de servicios de certificación. Para ello, éstos deberán emplear los elementos técnicos disponibles para brindar seguridad y privacidad a la información aportada, y los usuarios tendrán derecho a que se les informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elementos;

3°. A ser informado, antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, en su caso; de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso, y de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o que se convinieren;

4°. A que el prestador de servicios o quien homologue sus certificados le proporcionen la información sobre sus domicilios en Chile y sobre todos los medios a los que el usuario pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

5°. A ser informado, al menos con dos meses de anticipación, por los prestadores de servicios de certificación, del cese de su actividad, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 4° del artículo 16 de la presente ley, o bien, para que tomen conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;

6°. A ser informado inmediatamente de la cancelación de la inscripción en el registro de prestadores acreditados, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 3° del artículo 16 de la presente ley, o bien, para tomar conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;

7°. A traspasar sus datos a otro prestador de servicios de certificación;

8°. A que el prestador no proporcione más servicios y de otra calidad que los que haya pactado, y a no recibir publicidad comercial de ningún tipo por intermedio del prestador, salvo autorización expresa del usuario;

9°. A acceder, por medios electrónicos, al registro de prestadores acreditados que mantendrá la Entidad Acreditadora, y

10°. A ser indemnizado y hacer valer los seguros comprometidos, en conformidad con el artículo 14 de la presente ley.

Los usuarios gozarán de estos derechos, sin perjuicio de aquellos que deriven de la ley N° 19.628, sobre Protección de la Vida Privada y de la ley N° 19.496, sobre Protección a los Derechos de los Consumidores y podrán, con la salvedad de lo señalado en el número 10° de este artículo, ejercerlos conforme al procedimiento establecido en esa última normativa.

Artículo 24.- Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que éstos vayan cambiando.

TITULO VII

Reglamentos

Artículo 25.- El Presidente de la República reglamentará esta ley en el plazo de noventa días contados desde su publicación, mediante uno o más decretos supremos del Ministerio de Economía, Fomento y Reconstrucción, suscritos también por los Ministros de Transportes y Telecomunicaciones y Secretario General de la Presidencia.

Lo anterior es sin perjuicio de los demás reglamentos que corresponda aprobar, para dar cumplimiento a lo previsto en el artículo 10.

Artículo transitorio.- El mayor gasto que irroque a la Subsecretaría de Economía, Fomento y Reconstrucción las funciones que le asigna esta ley, durante el año 2002, se financiará con los recursos consultados en su presupuesto."

Habiéndose cumplido con lo establecido en el N° 1° del Artículo 82 de la Constitución Política de la República y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 25 de Marzo de 2002.- RICARDO LAGOS ESCOBAR, Presidente de la República.- Jorge Rodríguez Grossi, Ministro de Economía, Fomento y Reconstrucción.- Nicolás Eyzaguirre Guzmán, Ministro de Hacienda. Lo que transcribe para su conocimiento.- Saluda atentamente a usted, Álvaro Díaz Pérez, Subsecretario de Economía, Fomento y Reconstrucción.

Tribunal Constitucional.

Proyecto de ley sobre firma electrónica y los servicios de certificación de firma electrónica.

El Secretario del Tribunal Constitucional, quien suscribe, certifica que la Honorable Cámara de Diputados envió el proyecto de ley enunciado en el rubro, aprobado por el Congreso Nacional, a fin de que este Tribunal ejerciera el control de constitucionalidad respecto de su artículo 19, y por sentencia de 13 de marzo de 2002, lo declaró constitucional.

Santiago, Marzo 14 de 2002.- Rafael Larraín Cruz, Secretario.

II. REGLAMENTO DE LA LEY 19.799 SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y LA CERTIFICACION DE DICHA FIRMA.⁵⁵⁵

Núm.181.-Santiago, 9 de julio de 2002.- Vistos:

- a) Lo dispuesto en el artículo 32° N° 8 de la Constitución Política de la República;
- b) La ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma;
- c) Lo dispuesto en la resolución N° 520, de 1996, que fija el texto refundido, coordinado y sistematizado de la resolución N° 55, de 1992, ambas de la Contraloría General de la República.

Considerando: Que en fecha 12 de abril de 2002 se publicó en el Diario Oficial la ley N° 19.799 sobre documento electrónico, firma electrónica y la certificación de dicha firma, cuyo artículo 25 autoriza al Presidente de la República a dictar el reglamento correspondiente, en el plazo de 90 días contados desde la referida publicación, Decreto:

Artículo primero: Apruébase el siguiente Reglamento de la ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.

Artículo 1°. Los documentos electrónicos, la certificación y uso de la firma electrónica por las personas naturales y jurídicas de derecho privado y la administración del Estado, la prestación de los servicios de certificación, la acreditación de los certificadores, y los derechos y obligaciones de los usuarios se regirá por lo dispuesto en la ley N° 19.799, el presente Reglamento y las normas técnicas que se dicten al efecto.

TITULO PRIMERO

De los Prestadores de Servicios de Certificación

Artículo 2°. Son prestadores de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Son prestadores acreditados de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en Chile y acreditadas en conformidad con la Ley y este Reglamento, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Artículo 3°. El cumplimiento de las normas técnicas fijadas para la aplicación del presente Reglamento es obligatorio para los prestadores acreditados de servicios de certificación.

Artículo 4°. Los actos administrativos que impliquen la modificación de normas técnicas para la prestación del servicio establecerán los plazos en los cuales un prestador acreditado de servicios de certificación deberá adecuarse a las mismas. El incumplimiento en la adecuación a las nuevas normas técnicas será calificado como incumplimiento grave y facultará a la Entidad Acreditadora a dejar sin efecto la acreditación, de conformidad con el artículo 19 de la Ley y el presente Reglamento.

⁵⁵⁵ Publicado en el Diario Oficial el día 17 agosto 2002.

Artículo 5º. A petición de parte o de oficio, y con el objeto de fijar o modificar las normas técnicas establecidas por este Reglamento, la Entidad Acreditadora podrá iniciar el procedimiento para la elaboración y fijación de normas técnicas.

De ser necesario, se podrá fijar conjuntos alternativos de normas técnicas para la prestación del servicio con el objeto de permitir el uso de diversas tecnologías y medios electrónicos, en conformidad a la Ley y el presente Reglamento.

Artículo 6º. Es obligación de los prestadores de servicios de certificación contar con reglas sobre prácticas de certificación consistentes en una descripción detallada de las políticas, procedimientos y mecanismos que el certificador se obliga a cumplir en la prestación de sus servicios de certificación y homologación. Las Prácticas de Certificación deben declarar el cumplimiento de los requisitos señalados en el artículo 17 de este Reglamento, con excepción de la póliza de seguro que se acredita por medio de la presentación de la misma.

Las Prácticas de Certificación deben ser objetivas y no discriminatorias, y se deben comunicar a los usuarios de manera sencilla y en idioma castellano.

Dichas prácticas deberán contener al menos:

a. Una introducción, que deberá contener un resumen de las prácticas de certificación de que se trate, mencionando tanto la entidad que suscribe el documento, como el tipo de usuarios a los que son aplicables.

b. Consideraciones generales, debiendo contener información sobre obligaciones, responsabilidades, cumplimiento de auditorías, confidencialidad, y derechos de propiedad intelectual, con relación a todas las partes involucradas.

c. Identificación y autenticación, debiendo describirse tanto los procesos de autenticación aplicados a los solicitantes de certificados, como los procesos para autenticar a los mismos cuando piden suspensión o revocación de certificado.

d. Requerimientos operacionales, debiendo contener información operacional para los procesos de solicitud de certificado, emisión de certificados, suspensión y revocación de certificados, procesos de auditoría de seguridad, almacenamiento de información relevante, cambio de datos de creación de firma electrónica, superación de situaciones críticas, casos de fuerza mayor y caso fortuito, y procedimiento de término del servicio de certificación.

e. Controles de procedimiento, personal y físicos, debiendo describir los controles de seguridad no técnicos utilizados por el prestador de servicios de certificación para asegurar las funciones de generación de datos de creación de firma electrónica, autenticación de usuarios, emisión de certificados, suspensión y revocación de certificados, auditoría y almacenamiento de información relevante.

f. Controles de seguridad técnica, debiendo señalar las medidas de seguridad adoptadas por el prestador de servicios de certificación para proteger los datos de creación de su propia firma electrónica.

g. Perfiles de certificados y del registro de acceso público, debiendo especificar el formato del certificado y del registro de acceso público.

h. Especificaciones de administración de la política de certificación, debiendo señalar la forma en que la misma está contenida en la Práctica, los procedimientos para cambiar, publicar y notificar la política.

Artículo 7º. El prestador de servicios de certificación deberá mantener un registro de certificados de acceso público, en el que se garantice la disponibilidad de la información contenida en él de manera regular y continua.

A dicho registro se podrá acceder por medios electrónicos y en él deberán constar los certificados emitidos por el certificador, indicando si los mismos se encuentran vigentes, revocados, suspendidos, traspasados de otro prestador de servicios de certificación u homologados.

Artículo 8º. En caso que un prestador de servicios de certificación cese en la prestación del servicio, deberá comunicar tal situación a los titulares de los certificados por ella emitidos en la siguiente forma:

a) Si el cese es voluntario, con una antelación de a lo menos dos meses y señalando al titular que de no existir objeción a la transferencia de los certificados a otro prestador de servicios de certificación, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos. En este caso, si el prestador es acreditado, deberá traspasar los certificados, necesariamente, a un certificador acreditado.

b) Si el cese no es voluntario, la cancelación de la acreditación deberá comunicarse inmediatamente a los titulares. En caso que el prestador de servicios de certificación esté en situación de traspasar los certificados a otro prestador acreditado, deberá informar tal situación en la forma y plazo señalado en la letra a).

Si el titular del certificado se opone a la transferencia, el certificado quedará sin efecto sin más trámite, sin perjuicio de lo dispuesto en el artículo 11 de este Reglamento.

Artículo 9º. En caso que el cese en la prestación del servicio sea por voluntad del prestador acreditado de servicios de certificación, deberá solicitar a la Entidad Acreditadora, con al menos un mes de anticipación, la cancelación de su inscripción en el registro público a que hace referencia el artículo 16 de este Reglamento, comunicándole el destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferir y a quién, cuando proceda.

Artículo 10. El cese de la actividad del prestador acreditado de servicios de certificación será registrado como nota de cancelación de la inscripción de la acreditación por la Entidad Acreditadora en el registro público a que se refiere el artículo 16 de este Reglamento.

Artículo 11. Los datos proporcionados por el titular del certificado deberán ser conservados por el prestador de servicios de certificación a lo menos durante seis años desde la emisión inicial de los certificados, cualquiera sea el estado en que se encuentre el certificado.

En caso que el prestador de servicios de certificación cese en su actividad, deberá transferir dichos datos a un prestador de servicios de certificación, que deberá estar acreditado si aquel lo fuera, o a una empresa especializada en la custodia de datos electrónicos, por el tiempo faltante para completar los 6 años desde la emisión de cada certificado. Esta situación deberá verse reflejada en el registro público que señala el artículo 16 de este Reglamento.

Artículo 12. Los prestadores de servicios de certificación acreditados deberán contratar y mantener vigente un seguro de responsabilidad civil, que cubra los daños y perjuicios que ocasionen, con motivo de la certificación y homologación de firmas electrónicas, el que deberá contener las siguientes estipulaciones mínimas:

- a) Una suma asegurada de al menos el equivalente de cinco mil unidades de fomento;
- b) La ausencia de deducibles o franquicias, en la parte de la indemnización que no exceda el equivalente de cinco mil unidades de fomento;
- c) La responsabilidad civil asegurada, que comprenderá la originada en hechos acontecidos durante la vigencia de la póliza, no obstante sea reclamada con posterioridad a ella.

TITULO SEGUNDO

De la Acreditación de los Prestadores de Servicios de Certificación

Artículo 13. La acreditación es el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Entidad Acreditadora que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en la Ley y en este Reglamento, permitiendo su inscripción en el registro que se señala en el artículo 16.

Artículo 14. Las funciones correspondientes a la Entidad Acreditadora serán desarrolladas por la Subsecretaría de Economía, Fomento y Reconstrucción, la que, a efectos de su cumplimiento, podrá contratar expertos, a cuyos contratos se incorporarán normas sobre probidad administrativa.

Artículo 15. La Entidad Acreditadora ejercerá la facultad inspectora sobre los prestadores acreditados de servicios de certificación y, a tal efecto, velará porque los requisitos que se observaron al momento de otorgarse la acreditación y las obligaciones que impone la Ley y este Reglamento se cumplan durante la vigencia de la acreditación.

La facultad inspectora comprende tanto inspección ordinaria como la extraordinaria. La inspección ordinaria consiste en la facultad de practicar una visita anual a las instalaciones del prestador acreditado de servicios de certificación, como asimismo requerir, en forma semestral, información sobre el desarrollo de la actividad. La inspección extraordinaria será practicada de oficio o por denuncia motivada sobre la prestación del servicio, ordenada por el Subsecretario mediante resolución fundada.

Las inspecciones podrán ser practicadas por medio de funcionarios o peritos especialmente contratados y habilitados para estos fines, los que en el ejercicio de sus funciones podrán requerir al certificador información adicional a la proporcionada por él.

La información solicitada por la Entidad Acreditadora deberá ser proporcionada dentro del plazo de 5° día, contado desde la fecha de la solicitud, sin perjuicio del otorgamiento de plazos especiales atendida la información requerida.

Artículo 16. La Entidad Acreditadora mantendrá un registro público de prestadores acreditados de servicios de certificación, el que deberá contener el número de la resolución que concede la acreditación, el nombre o razón social del certificador, la dirección social, el nombre de su Representante Legal, el número de su teléfono, su sitio de dominio electrónico y correo electrónico así como la compañía de seguros con que ha contratado la póliza de seguros que exige el artículo 14 de la Ley.

El referido registro público deberá permitir su acceso por medios electrónicos, sin perjuicio de la mantención del mismo en soporte de papel en la Entidad Acreditadora. Este Registro deberá ser actualizado permanentemente, manteniendo un acceso regular y continuo.

Artículo 17. La acreditación es voluntaria, sin perjuicio de lo cual para obtenerla el prestador de servicios de certificación deberá cumplir, al menos, con las siguientes condiciones:

- a. Demostrar la fiabilidad necesaria de sus servicios.
- b. Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos.
- c. Emplear personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y gestión adecuados.
- d. Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación.
- e. Haber contratado un seguro apropiado en los términos que señala el artículo 12 de este Reglamento, y
- f. Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación.

El cumplimiento de dichas condiciones será evaluado por la Entidad Acreditadora de conformidad con las normas técnicas aplicables a la prestación del servicio, durante el procedimiento de acreditación.

Artículo 18. El procedimiento de acreditación de los prestadores de servicios de certificación se iniciará por medio de una solicitud presentada a la Entidad Acreditadora, acompañada del comprobante de pago de los costos de la acreditación y de los antecedentes que permitan verificar el cumplimiento de los requisitos de acreditación, con excepción de la póliza de seguro a que hace referencia el artículo 14 de la Ley.

En la solicitud que presente el interesado deberá individualizarse debidamente y para ello señalará su nombre o razón social, su RUT, el nombre y RUT del Representante Legal, su domicilio social y dirección de correo electrónico, aceptando expresamente dicho medio electrónico como forma de comunicación.

Artículo 19. Recibida la solicitud, la Entidad Acreditadora procederá a verificar la admisibilidad de la misma mediante la verificación de los antecedentes requeridos, dentro de 5° día hábil.

De ser inadmisibile la solicitud, dentro de 3° día hábil se procederá a comunicar al interesado tal situación, el que podrá completar los antecedentes dentro del plazo de 15 días, bajo apercibimiento de ser rechazada la solicitud.

Admitida a trámite la solicitud, la Entidad Acreditadora procederá a un examen sobre el cumplimiento de los requisitos y obligaciones exigidas por la Ley y este Reglamento para obtener la acreditación, certificando dentro del plazo de 90 días contados desde la fecha de la admisibilidad de la solicitud, prorrogables por una vez e igual período y por motivos fundados, que el interesado cumple los requisitos y obligaciones para ser acreditado y que dispone de un plazo de 20 días para presentar la póliza de seguros que exige el artículo 14 de la Ley, bajo apercibimiento de ser rechazada la solicitud.

Artículo 20. En caso que la Entidad Acreditadora determine que el prestador de servicios de certificación no cumple con las normas técnicas fijadas para el desarrollo de la actividad, señalará si los incumplimientos son subsanables, y si no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley para la firma electrónica avanzada.

En caso que los incumplimientos no sean subsanables, la Entidad Acreditadora procederá a dictar una resolución en la que rechaza la solicitud de acreditación.

Si los incumplimientos son subsanables y no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley para la firma electrónica avanzada, la Entidad Acreditadora podrá acreditar al interesado, previa autorización de un plan de medidas correctivas.

Artículo 21. Una vez completados los requisitos exigidos, la Entidad Acreditadora procederá a acreditar al interesado en el plazo de veinte días contados desde que, a petición del interesado, se certifique que la solicitud se encuentra en estado de resolverse.

Artículo 22. Durante todo el proceso de acreditación, la Entidad Acreditadora podrá solicitar documentación adicional y/o realizar visitas a las instalaciones del interesado, por intermedio de sus funcionarios o por expertos especialmente contratados para dichos fines.

Artículo 23. La acreditación del prestador de servicios de certificación producirá los siguientes efectos:

- a. La incorporación al registro público de prestadores acreditados que mantiene la Entidad Acreditadora.
- b. Habilitará al certificador a emitir certificados de firma electrónica avanzada.
- c. Someterá al certificador a la inspección de la Entidad Acreditadora.
- d. Los demás que establecen la Ley y este Reglamento.

Artículo 24. La Entidad Acreditadora por medio de resolución fijará dentro del primer trimestre de cada año el arancel de los costos de la acreditación y el arancel de supervisión.

Los costos de acreditación serán pagados por el prestador de servicios de certificación que solicite acreditarse, los que no serán restituidos en el evento que la acreditación no se conceda por incumplimiento de los requisitos y obligaciones legales y reglamentarias exigidos para el desarrollo de la actividad de certificación como acreditado.

El arancel de supervisión comprenderá los costos correspondientes a las inspecciones, ordinarias y extraordinarias, y del sistema de acreditación. El arancel deberá ser pagado por los prestadores acreditados de servicios de certificación dentro de los 90 días siguientes a la fecha de la resolución que los fija.

Artículo 25. La Entidad Acreditadora podrá dejar sin efecto la acreditación mediante resolución fundada, por las causales previstas en el artículo siguiente.

Dicha resolución deberá ordenar la cancelación de la inscripción del certificador del registro público que lleve la Entidad Acreditadora.

Artículo 26. La acreditación de los certificadores se dejará sin efecto por las siguientes causas:

a) Por solicitud del prestador acreditado de servicios de certificación, ante la Entidad Acreditadora con una antelación de a lo menos un mes a la fecha del término previsto por el prestador acreditado de servicios de certificación para que se haga efectiva, indicando el destino que dará a los certificados y a los datos de ellos, para lo cual deberá cumplir con lo dispuesto en el artículo 8 letra a) de este Reglamento, y garantizar el pago del aviso que deberá ser publicado de conformidad con lo dispuesto en el artículo siguiente.

b) Por pérdida de las condiciones que sirvieron de fundamento a su acreditación, la que será calificada por los funcionarios o expertos que la Entidad Acreditadora ocupe para el cumplimiento de la facultad inspectora.

c) Por incumplimiento grave o reiterado de las obligaciones que establece la Ley y este Reglamento.

En los casos de las letras b) y c), la resolución deberá ser adoptada previo traslado de cargos y audiencia del afectado, para lo cual la Entidad Acreditadora dará un plazo de 5 días hábiles para que éste evacue sus descargos. Recibidos éstos, la Entidad Acreditadora deberá resolver fundadamente dentro del plazo de 15 días, prorrogables por el mismo período por motivos fundados.

Artículo 27. Los certificadores cuya inscripción haya sido cancelada, deberán comunicar inmediatamente este hecho a los titulares de las firmas certificadas por ellos. Sin perjuicio de ello, la Entidad Acreditadora publicará, a costa del certificador, un aviso dando cuenta de la cancelación.

Dicho aviso deberá ser publicado en un medio de prensa escrito de circulación nacional, sin perjuicio de la publicación de la resolución en el registro público que señala el artículo 16 de este Reglamento. El aviso deberá señalar que desde esta publicación los certificados quedarán sin efecto, a menos que hayan sido transferidos a otro certificador acreditado.

TITULO TERCERO

De los Certificados de Firma Electrónica

Artículo 28. El certificado de firma electrónica es la certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de firma electrónica.

Los certificados de firma electrónica deben contener, al menos, las siguientes menciones:

- a. Un código de identificación único del certificado.
- b. Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada.
- c. Los datos de la identidad del titular, entre los cuales deben incluir su nombre, dirección de correo electrónico y su rol único tributario.
- d. Su plazo de vigencia.

Artículo 29. Los prestadores de servicios de certificación deberán introducir en los certificados de firma electrónica que emitan, las menciones señaladas en el artículo 15 de la Ley, de acuerdo con las normas fijadas por este Reglamento para el desarrollo de la actividad.

Los atributos adicionales que los prestadores de servicios de certificación introduzcan con la finalidad de incorporar límites al uso del certificado, no deberán dificultar o impedir la lectura de las menciones señaladas en el inciso anterior ni su reconocimiento por terceros.

Artículo 30. Tratándose de un certificado de firma electrónica avanzada, deberá el prestador de servicios de certificación comprobar fehacientemente la identidad del solicitante antes de la emisión del mismo, de conformidad con las normas técnicas.

Dicha comprobación la hará el prestador de servicios de certificación, ante sí o ante notario u oficial del Registro Civil, requiriendo la comparecencia personal y directa del solicitante o de su representante legal si se tratare de una persona jurídica.

Artículo 31. Los datos de creación de firma, cuando sean generados por el prestador de servicios de certificación, deben ser entregados al usuario o titular del certificado de manera de garantizar la recepción de los mismos en forma personal.

Queda prohibido al prestador de servicios de certificación mantener copia de los datos de creación de firma electrónica una vez que éstos hayan sido entregados a su titular, momento desde el cual éste comenzará a ser responsable de mantenerlos bajo su exclusivo control.

Artículo 32. El certificado de firma electrónica podrá ser usado por su titular de conformidad con las operaciones que han sido autorizadas a realizar en las prácticas de certificación del prestador de servicios de certificación con quien se ha contratado.

El certificado de firma electrónica avanzada deberá permitir a quien lo reciba verificar, en forma directa o mediante consulta electrónica, que ha sido emitido por un prestador acreditado de servicios de certificación, con la finalidad de comprobar la validez del mismo.

Artículo 33. Procederá la suspensión de la vigencia del certificado cuando se verifique alguna de las siguientes circunstancias:

- a. Solicitud del titular del certificado.
- b. Decisión del prestador de servicios de certificación en virtud de razones técnicas.

El efecto de la suspensión del certificado es el cese temporal de los efectos jurídicos del mismo conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del titular.

La suspensión del certificado terminará por cualquiera de las siguientes causas:

- a. Por la decisión del prestador de servicios de certificación de revocar el certificado, en los casos previstos en la Ley.
- b. Por la decisión del prestador de servicios de certificación de levantar la suspensión del certificado, una vez que cesen las causas técnicas que la originaron.
- c. Por la decisión del titular del certificado, cuando la suspensión haya sido solicitada por éste.

Artículo 34. Los certificados de firma electrónica quedarán sin efecto por la revocación practicada por el prestador de servicios de certificación.

La revocación tendrá lugar cuando el prestador de servicios de certificación constate alguna de las siguientes circunstancias:

- a) Solicitud del titular del certificado.
- b) Fallecimiento del titular o disolución de la persona jurídica que represente, en su caso.
- c) Resolución judicial ejecutoriada.

d) Que el titular del certificado al momento de solicitarlo no proporcionó los datos de la identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa.

e) Que el titular del certificado no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificador.

f) Que el titular del certificado no ha actualizado sus datos al cambiar éstos.

g) Las demás causas que convengan al prestador de servicios de certificación con el titular del certificado.

El efecto de la revocación del certificado es el cese permanente de los efectos jurídicos de éste conforme a los usos que le son propios e impide el uso legítimo del mismo.

Artículo 35. Los prestadores acreditados de servicios de certificación podrán homologar los certificados de firma electrónica avanzada emitidos por certificadores no establecidos en Chile, bajo su responsabilidad. Para ello el prestador acreditado de servicios de certificación deberá demostrar a la Entidad Acreditadora que los certificados por ella homologados han sido emitidos por un prestador de servicios de certificación no establecido en Chile que cumple con normas técnicas equivalentes a las establecidas en este Reglamento para el desarrollo de la actividad. Una vez practicada la homologación de un certificado o de un grupo de certificados de firma electrónica avanzada el prestador acreditado de servicios de certificación deberá, dentro del plazo de tercer día, comunicar tal situación a la Entidad Acreditadora y se deberá publicar, inmediatamente, en el registro de acceso público señalado en el artículo 7 de este Reglamento. Las prácticas de homologación deberán estar declaradas en las Prácticas de Certificación.

Artículo 36. La revocación de un certificado de firma electrónica podrá producirse de oficio o a petición de su titular por la concurrencia de algunas de las causales previstas en la Ley o en este Reglamento. La solicitud de suspensión o revocación, según corresponda, se podrá dirigir al prestador de servicios de certificación en cualquiera de las formas que prevean sus prácticas de certificación. La suspensión o revocación del certificado deberá ser comunicada inmediatamente a su titular, sin perjuicio que deba publicarse en el registro de acceso público que señala el artículo 7 de este Reglamento. Tratándose de la suspensión por razones técnicas o revocación del certificado de firma electrónica por las causales de las letras d), e) o f) del artículo 34, dicha decisión deberá ser comunicada al titular con anterioridad a su puesta en práctica, indicando la causa que la provoca y el momento en que se hará efectiva.

El término de la vigencia del certificado será oponible a terceros desde el momento de la publicación de ésta en el registro de acceso público que señala el artículo 7 de este Reglamento.

TITULO CUARTO

Protección de los derechos de los usuarios

Artículo 37. De acuerdo con el artículo 13 de la Ley el cumplimiento por parte de los prestadores no acreditados de servicios de certificación de las obligaciones que impone la Ley, en la forma que lo hacen los prestadores acreditados, servirá como antecedente para determinar la debida diligencia en la prestación del servicio, para los efectos de hacer efectiva la responsabilidad del artículo 14 de la Ley.

Artículo 38. De acuerdo con el artículo 23 de la Ley los usuarios podrán ejercer los derechos señalados en dicho artículo 23 de conformidad con el procedimiento establecido en la Ley 19.496 sobre protección de los derechos de los consumidores, salvo en lo que diga relación con el derecho a ser indemnizado y hacer valer los seguros comprometidos, situación en la cual se regirá por el derecho común.

TITULO QUINTO

Sobre la utilización de la firma electrónica por los órganos de la Administración del Estado

Párrafo 1º: Reglas comunes

Artículo 39. Los órganos de la Administración del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica.

Para tal efecto, los actos administrativos, formalizados por medio de documentos electrónicos y que consten en decretos o resoluciones, en acuerdos de órganos colegiados, así como la celebración de contratos, la emisión de cualquier otro documento que exprese la voluntad de un órgano o servicio público de la Administración del Estado en ejercicio de sus potestades legales y, en general, todo documento que revista la naturaleza de instrumento público o aquellos que deban producir los efectos jurídicos de éstos, deberán suscribirse mediante firma electrónica avanzada.

Artículo 40. La certificación de las firmas electrónicas avanzadas de las autoridades o funcionarios de los órganos y servicios públicos de la Administración del Estado se realizará por los respectivos ministros de fe. En aquellos órganos en que el ministro de fe no se encuentre expresamente establecido, el jefe superior del servicio deberá designar un funcionario público de planta, por resolución, para que actúe como certificador.

Artículo 41. Los órganos de la Administración del Estado podrán contratar, de acuerdo con las normas que rigen la contratación administrativa, los servicios de certificación de firma electrónica con un prestador acreditado de servicios de certificación, cuando mediante resolución fundada constaten su conveniencia técnica y económica. La estimación de dicha conveniencia estará basada en criterios de calidad de servicio y precio de éste.

Artículo 42. Los órganos de la Administración del Estado que utilicen documentos electrónicos deberán contar con un Repositorio o archivo electrónico a los efectos de su archivo una vez que haya finalizado su tramitación, de conformidad con las normas que regulan a su respectiva oficina de partes.

El Repositorio será responsabilidad del respectivo funcionario a cargo del archivo, sin perjuicio de la celebración de convenios de cooperación entre diferentes órganos o de la contratación de una empresa privada para que preste el servicio.

El Repositorio deberá garantizar que se respeten las normas sobre publicidad de los documentos, contenidas en la Ley 18.575 sobre Bases de la Administración del Estado y otras leyes especiales.

Artículo 43. El Repositorio deberá garantizar la seguridad, integridad y disponibilidad de la información en él contenida.

Para ello la información deberá ser respaldada en copias de seguridad, bajo las siguientes características:

a. La información deberá ser respaldada con cada proceso de actualización de documentos.

b. Se deberá mantener una copia de seguridad en el lugar de operación de los sistemas de información y otra en un centro de almacenamiento de datos electrónicos especializado. Este centro de almacenamiento de datos electrónicos, que puede ser propio o provisto por terceros, deberá cumplir con condiciones tales como un estricto control de acceso, un completo y detallado registro de entrada y salida de respaldos, resguardo de la humedad, temperatura adecuada, control del riesgo de incendio y otras.

c. El esquema de respaldo deberá ser simple, basado en generación de copias acumulativas, con el objeto de mantener la historia de la información en el mínimo de versiones posibles.

La seguridad, integridad y disponibilidad del Repositorio deberán estar caracterizadas por:

a. Medidas de seguridad y barreras de protección, frente al acceso no autorizado de usuarios.

b. Contar con monitoreo y alarmas que se activen cuando ocurra un evento no autorizado o fuera de programación, para el caso de eventuales fallas de las medidas de seguridad al acceso.

c. La sustitución de la información, por la versión más reciente que se disponga, en el menor tiempo posible, en casos de alteración no programada de aquella.

d. La existencia de un programa alternativo de acción que permita la restauración del servicio en el menor tiempo posible, en caso que el Repositorio deje de operar por razones no programadas.

Artículo 44. Para los efectos de garantizar la publicidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, los certificadores de los órganos y servicios públicos de la Administración del Estado deberán cumplir con normas técnicas equivalentes a aquellas fijadas para los prestadores de servicios de certificación acreditados para el desarrollo de la actividad.

Artículo 45. Los documentos electrónicos suscritos por medio de firma electrónica avanzada deberán contener un mecanismo que permita verificar la integridad y autenticidad de los mismos al ser impresos.

Artículo 46. La certificación de las firmas electrónicas avanzadas de las autoridades o funcionarios de los órganos y servicios públicos de la Administración del Estado deberá contener, además de las menciones propias de todo certificado, la fecha y hora de emisión del documento.

Artículo 47. Crease el Comité de Normas para el Documento Electrónico, cuya función principal será asesorar al Presidente de la República con respecto a la fijación de normas técnicas que deberán seguir los órganos de la Administración del Estado para garantizar la compatibilidad de los distintos tipos de documentos electrónicos.

Artículo 48. El Comité estará integrado por:

- a. El Ministro Secretaría General de la Presidencia, quien deberá presidirlo.
- b. El Subsecretario de Economía, Fomento y Reconstrucción.
- c. El Subsecretario de Telecomunicaciones.
- d. El Subsecretario de Hacienda.

Las labores de Secretaría Ejecutiva del Comité quedarán radicadas en el Subsecretario de Economía en su condición de titular de la Entidad Acreditadora.

Artículo 49. El Comité funcionará, en forma ordinaria, a lo menos dos veces al año, en los días y horas que acuerde. Su Presidente podrá citarlo a sesión extraordinaria cuando las necesidades del cumplimiento de su función así lo ameriten.

El Comité funcionará con la mayoría de sus integrantes y tomará los acuerdos por los dos tercios de sus miembros presentes.

Artículo 50. En el cumplimiento de su función, el Comité de Normas para el Documento Electrónico servirá de instancia de coordinación en las acciones de los Ministerios señalados en el artículo 48 de este decreto en el ámbito establecido en el artículo 47 y para ello estará facultado, si lo estima conveniente, para solicitar la asistencia de otros Ministros e invitar a otras autoridades.

Párrafo 2º: Sobre el uso de firmas electrónicas en la relación con los particulares

Artículo 51. Las personas podrán relacionarse con los órganos de la Administración del Estado a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito en la Ley y que tales técnicas y medios sean compatibles con los que utilicen dichos órganos.

Con la finalidad de garantizar dicha compatibilidad se estará a las normas técnicas fijadas a instancia del Comité creado en el artículo 47 del presente Reglamento.

Artículo 52. Las personas que se relacionen con la Administración del Estado por medios electrónicos, podrán utilizar firma electrónica, sin perjuicio de aquellos casos en que se haga necesaria la comprobación fehaciente de su identidad, en los cuales deberán emplear firma electrónica avanzada.

Artículo 53. Los órganos de la Administración del Estado podrán relacionarse por medios electrónicos con los particulares, cuando éstos hayan consentido expresamente en esta forma de comunicación.

Artículo 54. El Comité creado en el artículo 47, dentro del plazo de 90 días contados desde la fecha de entrada en vigencia del presente Reglamento, elaborará la

norma técnica que permita que las comunicaciones por medios electrónicos efectuadas entre los órganos de la Administración del Estado y de éstos con los ciudadanos operen de manera efectiva y eficiente.

Artículo 55. Lo dispuesto en este Título no se aplicará a las empresas públicas creadas por Ley, las que se registrarán por las normas previstas para la emisión de documentos y firmas electrónicas por particulares.

DISPOSICIONES TRANSITORIAS

Primera. En tanto no sean aprobadas las normas chilenas aplicables, se fijan como normas técnicas para todos los fines previstos en este Reglamento las siguientes:

Prácticas de Certificación:

- ETSI TS 102 042: “Policy requirements for certification authorities issuing public key certificates”.
- RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Marzo 1999.

Seguridad:

- ISO/IEC 17799:2000 Information Technology - Code of Practice for Information Security Management (2000).
- ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Version 2.1 (2000)
- FIPS PUB 140-1: Security Requirements for Cryptographic Modules (Mayo 2001).

Estructura de Certificados:

- ISO/IEC 9594-8:2001 “Information Technology - Open Systems Interconnection - The Directory attributr certificate framework”
- ITU-T Rec. X.690 (1997) / ISO/IEC 8825-1:1998. ASN.1 Basic Encoding Rules

Repositorio de Información:

- [RFC 2559] Boeyen, S. et al., “Internet X.509 Public Key Infrastructure. Operational Protocols - LDAPv2”, Abril 1999.

Segunda. Se define la siguiente gramática para incluir el RUT de empresas o personas en las extensiones ISSUER ALT NAME Y SUBJECT ALT NAME.

Según aparece en el documento de la IETF RFC 2594 la extensión Subject Alternative Name tiene la siguiente estructura (en formato ASN.1)

```
id-ce-subjectAltName OBJECT IDENTIFIER ::= {id-ce 17}
SubjectAltName ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
    otherName                [ OtherName,
                                0]
    /* otherName será el
    campo usado */
    rfc822Name                [ IA5String,
                                1]
    dNSName                   [ IA5String,
```

	2]	
x400Address	[ORAddress,
	3]	
directoryName	[Name,
	4]	
ediPartyName	[EDIPartyNam
	5]	e,
uniformResourceIdent	[IA5String,
ifier	6]	
iPAddress	[OCTET
	7]	STRING,
registeredID	[OBJECT
	8]	IDENTIFIER }

OtherName ::= SEQUENCE {
type-id OBJECT IDENTIFIER,
value [0] EXPLICIT ANY DEFINED BY type-id }

En este mismo documento se menciona que la opción “otherName”, es el lugar donde se deben especificar otro tipo de identificadores. Esta es la opción que se utilizará para almacenar el Rut.

Por lo tanto la información a almacenar será la siguiente:

SubjectAltName.otherName.Type-id = ““

SubjectAltName.otherName.Value = “99999999-D” (2 tipos de string : IA5String o PrintableString).

Tercera. La OID a usar por los prestadores de servicios de certificación será la siguiente:

Prefijo para PRIVATE ENTERPRISE NUMBERS: 1.3.6.1.4.1

Número asignado a la Entidad Acreditadora: 8321

Sufijos:

RUT del titular del certificado : 1

RUT de la certificadora emisora : 2

Por lo tanto, el OID completo para cada uno de estos ítems quedaría:

RUT del titular del certificado : 1.3.6.1.4.1.8321.1

RUT de la certificadora emisora : 1.3.6.1.4.1.8321.2

Artículo segundo. Derogase el decreto N° 81, de 1999, del Ministerio Secretaría General de la Presidencia.

Anótese, tómesese razón, comuníquese y publíquese.- RICARDO LAGOS ESCOBAR, Presidente de la República.- Jorge Rodríguez Grossi, Ministro de Economía, Fomento y Reconstrucción.- Javier Etcheberry Celhay, Ministro de Transportes y Telecomunicaciones.- Mario Fernández Baeza, Ministro Secretario General de la Presidencia.

Lo que transcribe para su conocimiento.- Saluda atentamente a usted.- Álvaro Díaz Pérez, Subsecretario de Economía, Fomento y Reconstrucción.
