

VALOR PROBATORIO DE LOS DOCUMENTOS

ELECTRÓNICOS

Introducción

Desde la invención de las primeras herramientas de piedra, el hombre ha confiado en la tecnología como una forma de ayudar a resolver problemas que se le presentan en la vida cotidiana. En aquellos primitivos tiempos, presenciamos el inicio de las comunicaciones (gestuales y verbales) así como también la aparición del comercio, entendido como el intercambio de bienes o servicios entre partes que consideraban estar recibiendo algo de igual o mayor valor, actividad que se consumaba en la forma de trueque.

De esta forma comienzan a edificarse comunidades de individuos que se agrupan en torno a recursos naturales que puedan consumir para su sobrevivencia. Casi inmediatamente se hace presente la necesidad de contar con un conjunto de reglas para vivir en armonía social, naciendo de esta manera el Derecho, entendido para nuestra introducción, como orden normativo de la conducta humana en sociedad, inspirado en principios de Justicia.

La evolución constante de la tecnología ha sido seguida de cerca en algunos casos, y con retraso en otros, por la normativa legal, que otorga validez, seguridad y garantía de cumplimiento a las relaciones comerciales entre particulares.

El avance aletargado que la tecnología tuvo hasta principios del siglo 18, contrasta con la celeridad en el desarrollo e invención de procesos y herramientas que se inician con la invención de la Maquina de Vapor Atmosférica en el año 1705, hecho que se considera como el inicio de la Revolución Industrial.

Sin embargo, aun tan magníficos logros pueden palidecer al ser comparados con la velocidad y complejidad con la cual se han desarrollado las comunicaciones electrónicas en los últimos 20 años.

Las Tecnologías de la Información (y Comunicaciones, según su acepción mas reciente) o IT, según sus siglas en inglés, (Information Technology), entendida en su concepto mas amplio puede ser definida como aquella actividad constituida por los desarrollos y aplicaciones de herramientas, maquinas y procedimientos que ayudan a procesar información. En particular el uso de computadoras y programas para convertir, guardar,

proteger, procesar, transmitir y recibir información, desde y hacia cualquier parte del planeta, en cualquier momento.

Esta facilidad en las comunicaciones globales permite que personas que se ubican en distintos puntos del planeta, aún sin conocerse, puedan establecer conexiones, contribuyendo, por lo tanto, al desarrollo de las relaciones comerciales y, por lo tanto, contractuales.

Si bien, entre un restringido número de empresas, la celebración de contratos por vía electrónica o telemática ya había venido desarrollándose desde hace décadas¹, éstas se basaban en un conocimiento recíproco, en la que la mutua confianza era el contrapeso frente a las inseguridades de carácter jurídico y técnicos², puesto que – como hemos señalado- la legislación necesaria para regular dichas relaciones, o bien no existía, o éstas se concebían en forma en precaria.

La necesidad de una regulación uniforme sobre la materia fue visualizada por la Asamblea General de Naciones Unidas, que en el año 1966 creó la Comisión de las Naciones Unidas para el

¹ Por ejemplo, la transferencia bancaria de fondos o contratación bursátil.

² Inseguridades que eran previamente minimizadas mediante la adopción de medidas de seguridad y la suscripción de un convenio normativo que amparara las fórmulas de contratación.

Derecho Mercantil Internacional (UNCITRAL, por sus siglas en inglés) que ***es el órgano jurídico central del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional.*** En el cumplimiento de su misión de fomentar la armonización y la unificación progresivas del derecho mercantil internacional, en particular en el área relativa a Comercio Electrónico destaca redacción de la Ley Modelo de la UNCITRAL sobre Comercio Electrónico. Esta ley, elaborada en el año de 1996, tiene por objeto facilitar el uso de medios modernos de comunicación y de almacenamiento de información, por ejemplo el intercambio electrónico de datos (EDI), el correo electrónico y la telecopia, con o sin soporte de Internet. De acuerdo con la Comisión, la Ley Modelo se basa en el establecimiento de un equivalente funcional de conceptos conocidos en el tráfico que se opera sobre papel, como serían los conceptos "escrito", "firma" y "original".

Ya han sido varios países, los que han implementado una normativa legal para regularizar y permitir la utilización cotidiana, ágil y diligente, de medios tecnológicos en la formación del consentimiento de los contratos. Estas legislaciones se han basado

en los principios inspiradores de la Ley Modelo, como son la **equivalencia funcional** entre el documento con soporte de papel y el documento electrónico, y el de la firma autógrafa y la firma electrónica, el principio de la **neutralidad tecnológica**, y el principio de la **actuación de buena fe** en las relaciones que se establecen a través del empleo de medios electrónicos.³

En Estados Unidos, el año 1995, se dictó la primera ley, la *Utah Digital Signature Act*, que ha regulado los aspectos jurídicos de la forma digital como instrumento probatorio. Posteriormente surgieron proyectos legislativos en Georgia, California y Washington. En Europa, el primer país que elaboró una ley de firma digital, ha sido Alemania, la que la aprobó el 13 de Junio de 1997.

México modificó y adicionó sus códigos Civil y de Comercio en el año 2000. Las modificaciones del Código Civil introducen el principio de la equivalencia funcional, al validar el consentimiento que haya sido otorgado en forma electrónica. Las adiciones al

³ Con respecto a los principios generales en que se basa la Ley Modelo, cabe tener en cuenta la siguiente lista no exhaustiva: 1) facilitar el comercio electrónico en el interior y más allá de las fronteras nacionales; 2) validar las operaciones efectuadas por medio de las nuevas tecnologías de la información; 3) fomentar y estimular la aplicación de nuevas tecnologías de la información; 4) promover la uniformidad del derecho aplicable en la materia; y 5) apoyar las nuevas prácticas comerciales.

Código de Comercio serán vistas en detalle en las siguientes páginas.

En nuestro país, el día 12 de Abril de 2002, se publicó en el Diario Oficial la Ley N° 19.799, sobre *“Documentos Electrónicos, firma electrónica y servicios de certificación de dicha firma”*. En el mensaje con que el Ejecutivo acompañó la referida ley, dice que: *“es necesario un marco legal en que actos y contratos celebrados por medios electrónicos tengan la misma validez y protección ante la ley que los celebrados de manera convencional.”*

Es evidente que la eficacia de estas leyes radica en su uniformidad en los estándares mínimos referidos, ya que si su contenido difiere en cada país, será difícil su aplicación a un entorno global, lo cual al momento de la interpretación puede acarrear serios problemas, sobre todo a los jueces que deban determinar la validez de una firma o certificado extranjero al tiempo de un litigio.

Para ello no es menester, de hecho, conocer a fondo la tecnología existente, porque de así hacerlo, los legisladores y juristas deberían ser científicos y su trabajo perdería todo valor normativo, pero si es necesaria una preparación mínima a fin de

esclarecer al menos los conceptos generales que rigen en materia técnica para poder subsumirlos en el ámbito de las normas vigentes o por aprobar.

Con la entrada en vigencia de la referida ley 19.799, se reconoce pleno valor al documento que ha sido suscrito mediante la llamada “firma electrónica”, equiparándolo al documento “tradicional”, hecho que aún es desconocido para la gran mayoría de los chilenos, entre los que todavía existe cierta desconfianza hacia éstos instrumentos, sobre todo en lo relativo a sí estos tienen algún valor jurídico para probar lo que ahí se consigna; puesto que –según imagina una buena parte de la población- los jueces son personas ajenas a la computación y/o Internet.

Nada más lejos de la realidad puesto que, no sólo a los jueces actuales se les exige que tengan conocimientos de computación, a nivel de usuario, sino que –además y más importante aún- es la propia ley la que despejó el asunto al disponer, expresamente, *que la firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio que los documentos electrónicos que tengan la calidad*

*de instrumento público, deberán suscribirse mediante **firma electrónica avanzada***⁴

Es más, la propia Ley regula, incluso, el valor probatorio de los mismos, dado que en su artículo 5° establece las reglas para que los documentos electrónicos puedan ser usados como medio de prueba en juicio, disponiendo que: “**1.-** Los documentos electrónicos que tengan la calidad de instrumento público, harán plena prueba de acuerdo con las reglas generales; y **2.-** Los que posean la calidad de instrumento privado, en cuanto hayan sido suscritos mediante firma electrónica avanzada, harán plena prueba de acuerdo con las reglas generales. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales.”

Sin duda, es un gran avance si tradicionalmente hemos tenido una gran desconfianza hacia cualquier cosa que no sea la escritura en que no haya intervenido un Notario Público, erigiéndose éste – para el común de los ciudadanos- como el Ministro de Fe por excelencia, único medio probatorio fehaciente e indubitable.

⁴ Artículo 4 de la Ley 19.799.

Esta memoria pretende contribuir al fortalecimiento de los documentos electrónicos como medios válidos tanto para la formación del consentimiento, como para dar fe de los hechos en que ahí se consignan.

En este mismo orden de ideas, hemos advertido que, por una parte, la actual legislación, a nuestro juicio, carece de la precisión que sí tiene el Código de Comercio Mexicano que regula en detalle y exhaustivamente, no sólo el valor probatorio de los contratos electrónicos, sino que también vela por los aspectos relativos a la formación del consentimiento, detalle que no es menor, puesto que ello determina el factor de competencia relativa (territorio), como la legislación vigente; y, por la otra, aún existe cierta resistencia en otorgarle pleno valor probatorio, a documentos o certificados electrónicos.

El objetivo de esta memoria, es contribuir a la correcta evaluación del documento electrónico y arrojar alguna luz en cuanto a su valor probatorio, tanto bajo un prisma técnico como legal, y dentro de este último, con la ayuda de la comparación con la legislación mexicana, con el fin de sugerir, si fuere procedente, eventuales aspectos que debieran perfeccionarse.

Para ello, se entregará al lector un marco teórico acerca de la contratación electrónica y la prueba de dichos contratos; luego, se analizará la problemática jurídica que plantea el valor probatorio de los documentos electrónicos, esto es la integridad y autenticidad de éstos, a la luz de la legislación chilena y de la legislación mexicana, la que modificó su Código de Comercio en el año 2003, en relación a la contratación electrónica. Concretamente, se plantea la dificultad de probar la fidelidad del contenido de los documentos electrónicos, y la eficacia probatoria de la firma electrónica, a fin de determinar su autoría o atribuir responsabilidades.

1er. Capítulo: De la Internet y el Documento Electrónico

1. Que es Internet.

Internet, “La red de redes”, o “superautopista de la información” como también se le conoce, es un sistema mundial de redes computacionales interconectadas entre ellas por el conjunto de protocolos de comunicación TCP/IP (Transmission Control Protocol TCP y el Internet Protocol IP), y que puede ser accesada públicamente. Está compuesta por miles de redes, sean estas comerciales, académicas, gubernamentales, militares, particulares, etcétera. Transporta información y servicios de varios tipos, como acceso remoto a otras máquinas (telnet y ssh), transferencia de archivos (FTP), correo electrónico (e-mail), boletines electrónicos (news o grupos de noticias), conversaciones en línea (chat), mensajería instantánea (ICQ, MSN, IM). Al contrario de lo que se piensa comúnmente, Internet no es sinónimo de World Wide Web (www). Ésta es parte de aquella, siendo la World Wide Web uno de los muchos servicios ofertados en la red Internet.

Sus orígenes se remontan a finales de la década de los 60, cuando la Agencia de Proyectos de Desarrollo Avanzado del Departamento de Defensa de los Estados Unidos de Norteamérica

(DARPA, por sus siglas en inglés) creó ARPANET, la primera red basada en un sistema descentralizado de organización y administración, lo que cumplía los requerimientos del Gobierno de Estados Unidos, que buscaba un sistema de comunicaciones redundante y que pudiera subsistir en caso de un ataque nuclear. En el año 1983 ARPANET cambió su sistema de protocolos de comunicación desde NCP (siglas en inglés para Network Control Protocol) a TCP/IP, lo que establece el punto de partida de la Internet como la conocemos hoy en día.

A principios de los años 90s se creó el Lenguaje de Marcación de Hipertexto, o HTML por sus siglas en inglés, una particular forma de codificar un texto, en el cual las atributos del mismo (como su color, posición, fuentes, estructura, etc.) están incluidas en el texto final, de tal forma que es posible para un programa especializado (el navegador de internet o “Browser”) desplegar las paginas tal y como fueron concebidas por su autor. Esto dio inicio al World Wide Web (www) o “telaraña mundial” sin lugar a dudas, la cara mas conocida de la Internet. A partir de ese momento el uso de Internet he crecido en forma casi exponencial.

2. Documento Electrónico.

Por documento electrónico, podemos intentar una definición, a modo general, que se trata de información o datos (que no sean programas o archivos de sistema) contenidos o registrados en medios electrónicos, los que permiten su almacenamiento y posterior uso sin necesidad de que dicha información o datos sean impresos (no obstante a que generalmente la impresión es posible).

Durante largo tiempo se consideró que la información contenida en una computadora era algo interno e intangible que hacia necesario la impresión de dicha información en el soporte papel para poder proceder correctamente con su uso. En la actualidad, gracias al desarrollo de las redes computacionales, y en particular a Internet, resulta más conveniente realizar la distribución de documentos electrónicos que la de sus pares impresos. (Esta memoria de grado es una prueba patente, pues fue íntegramente editada y corregida mediante el intercambio de documentos electrónicos, encontrándose su autor en Norteamérica y luego en Europa, en tanto que las correcciones y presentación final fueron hechas en Chile.) No obstante lo anterior, la utilización de documentos electrónicos ha creado nuevos problemas que no

presenta el papel, como la perdurabilidad y la compatibilidad de formato para la lectura del documento, al tiempo que comparte los problemas de seguridad, fidelidad al igual que el papel, aunque en este caso, estos problemas deben ser resueltos bajo una perspectiva muy distinta.

Los problemas de *perdurabilidad* del documento electrónico, dicen relación, ya a los medios mismos en los cuales se almacena la información (discos flexibles, unidades de disco rígido, unidades de memoria Flash, CDroms, etc) medios que tienen una marcada tendencia a la obsolescencia (por ejemplo, las unidades de discos flexibles fueron en principio de un formato de 12,5 pulgadas, para convertirse luego en 5,25 pulgadas, luego en 3,5 pulgadas o FloppyDisks, mismos que ya no son incluidos en computadoras modernas, el DVD que esta desplazando al CDRom, etc), sin dejar de observar que ninguno de estos medios ha existido por mas de medio siglo, lo que lleva a preguntarnos, como pueden compararse con el soporte papel, que en su caso mas extremo, como en lo los papiros egipcios, ha sobrevivido y guardado información por mas de 3 milenios. Las funciones del documento electrónico con fines de archivo están aun en una fase incipiente de discusión.

El problema de *incompatibilidad* del formato dice relación con la forma particular de codificar la información para su respaldo en un archivo de computadora. En sí, las computadoras, y sus medios de almacenamiento, solo pueden almacenar bits, que es la unidad de información más básica, que representa uno de dos posibles estados, verdadero o falso, encendido o apagado, o en su representación binaria, 0 y 1. Por lo tanto, para almacenar información en una computadora, disco duro, o red, es necesario “convertir” la información en 0s y 1s, y viceversa. Cada programa de computadora tiene su propia forma de codificar información, es mas, diferentes versiones de un mismo programa pueden codificar información de manera distinta. Este problema puede ser resuelto utilizando formatos de archivo que sean estándares públicos (o formatos abiertos), como XML, HTML, PNG, etc., sin embargo es de notar que no siempre se utilizan formatos abiertos, siendo el caso mas prominente el formato utilizado por Microsoft Word, el cual es confidencial, por lo que, en teoría Word y solo Word puede leer archivos de Word, y solo los programadores de Microsoft saben como codificar y decodificar correctamente un documento de Word.

Estos temas han sido mencionados someramente para ejemplificar otros tantos puntos controversiales que existen sobre el documento electrónico, pero siendo estos de un alcance más técnico, escapan por el momento, a la atención de esta memoria.

La Ley 19.799 del 12 de abril de 2002 define el documento electrónico en su artículo 2do, letra d), a saber; 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.

Será en este contexto que se analizará su valor probatorio a la luz de la legislación actual.

3. De los contratos, en general, a la especificación de los contratos electrónicos.

En nuestro ordenamiento jurídico privado, rige el principio de Autonomía de la Voluntad, consagrado en el artículo 1545 del Código Civil⁵, bastando que las partes hayan prestado su consentimiento en la realización de un acto jurídico, y que el objeto

⁵ “Todo contrato legalmente celebrado es una ley para los contratantes, y no puede ser invalidado sino por su consentimiento mutuo o por causas legales.” Artículo 1545 Código Civil.

y la causa de la misma sean lícitos. Será el Código de Comercio la que regula la forma en que alcanza el consentimiento, mediante la oferta y aceptación.

El contrato celebrado, atendida su naturaleza, se perfeccionará, ya sea mediante el sólo consentimiento, ya sea mediante la entrega, ya sea mediante el cumplimiento de las formalidades; y, la prueba acerca de la celebración del convenio, así como también, de los términos de éste, se realizará de acuerdo a las reglas generales, teniendo gran relevancia, si éste contrato tiene, a lo menos, algún principio de prueba por escrito. Regla que, por cierto, también debe aplicarse a los contratos electrónicos o telemáticos, los que podrían definirse como *acuerdo de voluntades con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática*.

En efecto, en principio, y sin perjuicio de su posterior prueba, todo contrato sería susceptible de perfeccionamiento por medios electrónicos, siempre que cumpla con los requisitos de validez, obligando no sólo a lo pactado sino también a las consecuencias que de él se derivan.

La excepción a la regla general, está en los contratos que para su perfeccionamiento deben de ir revestidos de ciertas solemnidades, o que lo hagan mediante la entrega, no siendo susceptibles de hacerlo por vía electrónica⁶.

En estos casos, sin embargo, no se ve dificultad alguna para que las partes lleguen a un acuerdo vía electrónica, pero para la formalización y validez del contrato, deberían cumplirse con las demás exigencias del Código Civil, siendo de alta conveniencia de un consentimiento preventivo a una forma de contratación no expresamente prevista en el ordenamiento, ni socialmente tenida como tal, en la utilidad que para las partes representa el que su interlocutor asuma las responsabilidades derivadas del empleo del medio y en la ventaja que supone el diseño de un esquema de distribución de riesgos.

En el Derecho Comparado, el legislador español, del siglo XIX, ya había sometido la validez de los contratos concertados por telégrafo, a la previa admisión expresa por las partes de ese medio en documento escrito y, además, si así se hubiera pactado, a que los telegramas reunieran las condiciones o signos convencionales

⁶ Como por ejemplo la tradición, el otorgamiento de testamento, las capitulaciones matrimoniales, la celebración de matrimonios, etcétera.

acordados. Esta misma solución fue adoptada por la doctrina española, condicionando la posibilidad de celebrar contratos por medios electrónicos a la previa existencia de un convenio normativo entre los contratantes, en el que se reconozca la aptitud declarativa de las futuras transmisiones de actos jurídicos, se asuman preventivamente sus consecuencias y, en su caso, se distribuyan o modalicen los riesgos que el procedimiento genera.⁷

4. Acerca de la prueba de los contratos electrónicos.

La particularidad distintiva de los contratos concluidos por medios electrónicos o telemáticos, a través del envío de mensajes recíprocos entre las partes, se encuentra en el vehículo utilizado para la emisión de las correspondientes declaraciones de voluntad, circunstancia de la que derivan los condicionamientos para su admisión y las peculiaridades de su régimen probatorio.

Esto por cuanto las comunicaciones electrónicas se encuentran aquejadas – a primera vista- de un evidente problema de inseguridad, tanto en lo que afecta a la imputabilidad de su

⁷ Bonardell Lenzano, Rafael, “La contratación electrónica en el ordenamiento jurídico español y perspectiva de armonización europea: el borrador de directiva sobre sistemas de firma electrónica”, página 4.

contenido a un determinado sujeto (*autenticidad*), como a la *integridad* del mismo, frente a eventuales alteraciones.

Este defecto puede constituir una incapacidad original del procedimiento para la conclusión de contratos, pues la dificultad para establecer una vigorosa presunción de procedencia, impidiendo contar, en numerosos casos, con un sujeto a quien atribuir la declaración de voluntad, determina la inexistencia del negocio, puesto que los documentos en cuestión no se encuentran firmados.

No obstante esa inhabilidad inicial, existen procedimientos para dotar de fiabilidad a estas transmisiones, las ciencias tecnológicas han debido idear sistemas para otorgar la confianza necesaria a los usuarios que pretenden acceder a la contratación electrónica, medidas que han sido respaldadas, luego, por las legislaciones, tanto de nuestra nación, como a nivel internacional.

Tanto la Ley chilena, como la mexicana, ha consagrado en sus textos legales, los principios que los han inspirados, resultando revisarlos someramente.

5. Principios que informan las legislaciones chilenas y Mexicana en relación a los documentos electrónicos.

Nuestra ley N° 19.799 se inspiró en los principios de: libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional; y, equivalencia del soporte electrónico al soporte de papel.

Por su parte, México funda su normativa en los principios de neutralidad tecnológica; autonomía de la voluntad: compatibilidad internacional; equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa.

De la mera comparación, es posible constatar que ambas legislaciones comparten los principios de neutralidad tecnológica, compatibilidad internacional y equivalencia funcional, los que se refieren a:

La neutralidad tecnológica: implica que la ley debe ser neutra respecto de la tecnología, es decir, no debe hallarse atada a una tecnología de firma electrónica en particular, si pretende legislar y seguir vigente a futuro, a pesar de que los medios

utilizados para la identificación de personas o validación de documentos puedan variar⁸;

La compatibilidad internacional: dice relación, genéricamente, a la compatibilidad de los programas o software utilizado para la creación de las firmas electrónicas y su registro, a fin de permitir que las operaciones internacionales de comercio por vías electrónicas mantengan un mínimo de seguridad jurídica que permita su desarrollo a través del reconocimiento de las firmas electrónicas generadas en distintos países; ⁹ y,

La equivalencia funcional:

No obstante la diferente enunciación, nuestro principio de **“equivalencia del soporte electrónico al soporte de papel”**, no es otro que **“La equivalencia funcional del Mensaje de**

⁸ Al citar este principio, que ya se encuentra en muchas legislaciones, lo que se intenta es evitar el ejemplo de la Ley española de tarjetas magnéticas, la cual quedó obsoleta al momento de ser promulgada, pues las tarjetas de banda magnética ya habían dado paso a las nuevas tarjetas de microchip que actualmente se utilizan en Europa.

⁹ En México, el Capítulo VI, artículo 114, define expresamente el reconocimiento internacional de los certificados a fin de mantener la seguridad jurídica de las transacciones internacionales. Por su parte la Ley 19.799 en su artículo 15 inciso 2º. Dispone que: 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 o que se encuentre vigente.

Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa”, consagrada en México, la que resulta indispensable a fin de crear verdadera seguridad jurídica en el uso habitual de los medios informáticos y telemáticos para la realización de operaciones comerciales, y que se analizará en extenso más adelante.

La **autonomía de la voluntad**, consagrada expresamente en México como principio rector de las modificaciones efectuadas al Código de Comercio del mencionado país, es en el nuestro, principio general del derecho privado, razón por la cual no requirió consagrarla precisa y claramente.

Por nuestra parte, los principios de **libertad de prestación de servicios** y **libre competencia**, son consecuencia de nuestro sistema económico imperante.

6.- Definición legal de Documento electrónico.

El artículo 2, letra d), de la Ley 19.799 define documento electrónico como: *“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”.

El Código de Comercio mexicano no define documento electrónico como tal, sino como “**mensaje de datos**”, entendiéndolo por ello lo siguiente: “*La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología*”.¹⁰ Como es posible de apreciar esta definición se aproxima más a la de documento electrónico, puesto que en rigor, mensaje de datos es aquél que está destinado a su transmisión.

7. Valor probatorio de los documentos electrónicos.

Sin perjuicio que la reina de las pruebas sea la confesión, el método más extendido para probar la existencia de un contrato previo celebrado entre las partes, en circunstancias que una de éstas pretenda desconocerla, es a través de la prueba documental.¹¹

La prueba documental o instrumental es la que se produce por medio de documentos o instrumentos en la forma prefijada por las leyes, y es la de mayor uso en el mundo contractual y mercantil.

¹⁰ Artículo 89.

¹¹ Importante es recordar que los actos o contratos que contengan la entrega o promesa de una cosa que valga más de dos unidades tributarias, deben constar por escrito, según el artículo 1709 del Código Civil Chileno.

El documento goza de gran confianza para el legislador en atención a la fijeza que da al hecho a probar.

En términos amplios debe entenderse por **documento o instrumento** a cualquier objeto que contenga 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.

Los elementos propios de esta noción amplia son la existencia de un soporte en que constan, un medio que se emplea para grabar los signos, un lenguaje o idioma y un mensaje o "contenido".

En un sentido restringido, con la expresión documento sólo se reconocen a aquellos que están escritos en soporte papel y rubricados o firmados manualmente. Y, documento electrónico, como se ha dicho, es *“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”*.

Si analizamos la noción tradicional de documento referida al instrumento en el que queda plasmado un hecho que se exterioriza

mediante signos materiales y permanentes del lenguaje, vemos como el documento electrónico cumple con los requisitos del documento en soporte de papel en el sentido de que contiene un mensaje (*texto alfanumérico o diseño gráfico*) en lenguaje convencional (*el de los bits*) sobre soporte (*cinta o disco*), destinado a durar en el tiempo.

Los documentos soportados en medios magnéticos no responden al concepto tradicional o restringido de documento manuscrito en soporte en papel, sino al amplio.

Al hablarse de documentos electrónicos se alude a casos en que el lenguaje binario -sobre un soporte magnético/óptico - constituye la acreditación, materialización o documentación de una voluntad quizás 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 magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque sólo pueden ser leídos o conocidos por el

hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales.¹²

Los documentos electrónicos poseen los mismos elementos que un documento escrito en soporte papel:

a) constan en un **soporte material** (cintas magnéticas, discos flexibles o rígidos, discos magneto-ópticos, discos ópticos, chips de memoria, memoria tipo Flash, etc.)¹³;

b) contiene un **mensaje**, el que está codificado para su correcto almacenamiento en medios digitales, usando el lenguaje binario o bits, en entidades magnéticas que los sentidos humanos no pueden percibir directamente;

c) están escritos en un **idioma** o código determinado; y,

d) pueden ser **atribuidos** a una persona determinada en calidad de autor mediante una firma digital, clave o llave electrónica.

¹² Por exclusión, entendemos que constituye un documento no electrónico aquel que es elaborado por las formas tradicionales, sean éstas manuales, mecanográficas, micrograbadas, microcopiadas o fotográficas.

¹³ Por una cuestión práctica, eventualmente será necesario imprimir o traspasar a soporte en papel los documentos digitales o electrónicos; como ocurre con, por ejemplo, las declaraciones aduaneras de importación de mercancías que deben imprimirse para retirar las mercancías desde los recintos portuarios o para pagar en los bancos los derechos de aduana.

De lo anterior, y en relación al valor probatorio de los mencionados documentos electrónicos, necesario es establecer la fidedignidad del mensaje contenido en éste, y la autenticidad de la firma digital, si lo hubiere, o la comprobación por otros medios, de la identidad del autor del mensaje.

2do. Capitulo: Problemática Jurídica Del Valor

Probatorio De Los Documentos Electrónicos.

8.- Planteamiento del problema.

En relación a los documentos electrónicos, y el valor probatorio de que están dotados, surge un **primer problema** cual es **la fidedignidad del contenido de los documentos electrónicos.**

Además, como segunda cuestión en torno al cual se centra la problemática del valor probatorio de los documentos, dice relación a que la firma digital de los documentos electrónicos puede no existir, y al no intervenir el hombre carecerá de firma manuscrita y será difícil determinar su autoría o atribuir responsabilidades.

Sin perjuicio que ambas cuestiones se encuentran estrechamente relacionados, serán analizadas por separado. Ahora veremos la autenticidad del documento electrónico, modo en que puede ser subsanado la falta de firma autógrafa.

9.-Análisis del problema planteado, nociones preliminares de la firma:

La importancia de la firma no es menor, puesto que cualquier documento no firmado puede ser fácilmente desechado de los procesos judiciales, pues la simple falta de este elemento transforma cualquier documento en simple indicio (*en caso de ser usado como prueba*) o le quita todo valor jurídico, si es emanado de autoridad judicial, al ser la firma un requisito de toda resolución judicial, debido a que sólo así otorga seguridad jurídica, ya que de otra manera resultaría imposible vincular el documento a cualquier Juez en ejercicio de sus funciones, garantía básica del Estado de Derecho.

Necesario es, por lo tanto, realizar una descripción de los caracteres jurídicos y de las funciones legales y sociales de la firma para luego contemplar el ámbito normativo que la rige y la posible adaptabilidad de la nueva legislación a esos conceptos.

10. Categorías de firmas.

La firma se puede separar en dos grandes grupos o categorías¹⁴:

I. **Firma Autógrafo:** Es un trazado gráfico que habitualmente contiene el nombre, apellido y la rúbrica de una persona, mediante el cual se suscriben los documentos para darle autoría y obligarse a cumplir con lo que en ellos se dice. De forma más simple, se ha dicho que es el conjunto de letras o signos que identifican a la persona que la estampa en un documento o texto.

II. **Firma no Autógrafo:** es toda aquella realizada por cualquier otro medio que no sea la inscripción manual de los rasgos que identifican a una persona. En esta categoría podemos incluir, por ejemplo, a la firma digital, a la electrónica y cualquier otra realizada por medios técnicos o de cualquier otra especie.

11. Referencias históricas:

¹⁴ Sin perjuicio de lo anterior, existen algunos tipos especiales de firma: (a) Firma a ruego: Es aquella en la cual persona distinta de quien suscribe firma por quien desea avalar el documento en cuestión a fin de otorgar al mismo certeza jurídica. Por regla general la utilizan las personas que no saben o no pueden firmar por impedimento específico, lo cual no implica necesariamente en todos los casos que aquél que solicita la misma no pueda o no sepa leer, lo cual aunado al hecho de que el notario puede leer el documento por o para el firmante otorga pleno valor a los actos así realizados; y, (b) Firma de letrado: Requisito procesal de la mayoría de las legislaciones, que implica la existencia del patrocinio en el procedimiento escrito, y hace responsable al letrado que firma por el contenido del escrito presentado ante autoridad competente y, en su caso, de las posibles sanciones que pudieren corresponder cuando se actúa por fuera de lo establecido por la ley o las prácticas profesionales vigentes.

Sin soslayar su actual importancia, debemos reconocer que la aparición de la firma es relativamente reciente. En Roma, base de nuestro sistema jurídico, no era costumbre firmar los documentos. La *manufirmitio* (ceremonia de validación del contenido de los documentos) consistía en que, habiendo sido leído el documento por su autor o el notario, se lo colocaba desplegado sobre la mesa del fedatario interviniente y, luego de pasar la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo, se escribía el nombre, o una o tres cruces, por el autor o el notario en su nombre, y luego por los testigos si los hubiere.

Aun a pesar de la descripción solemne que se otorga, la *manufirmitio* no era en verdad un requisito del acto, sino mas bien parte del procedimiento actuado que, en la mayoría de los casos, caracterizó las transacciones romanas; pero el hecho de poder estamparse cruces en lugar de los nombres en realidad nos da idea de la poca importancia en sí de la firma como hoy la conocemos.

12. Definición de firma:

A falta de definición legal, debemos remitirnos a las definiciones aceptadas por el Diccionario de la Real Academia Española respecto de la firma, de las cuales hemos descartados

intencionalmente aquellas no referidas a la firma como elemento integrante de un documento debido a la exposición previa sobre las funciones de la firma: ***“Firma. Nombre y apellido que una persona pone, con rúbrica o sin ella, al pie de un escrito como señal de autenticidad.”***

La definición presentada acepta la idea de lo que es la firma en su significado lato sensu, pero los tratadistas Planiol y Ripert la definen de la siguiente manera: *“la firma es una inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto”*.¹⁵

13. Funciones de la firma:

La firma como tal, no es más que una nueva modalidad de avalar documentos, tanto en el significado lego como en el jurídico; y, para extrapolar los efectos jurídicos de una firma tradicional al campo de la electrónica útil es describir las funciones de la primera de las firmas mencionadas para luego analizar la factibilidad del objetivo propuesto, las que son:

1º Identificación: porque la firma en sí misma identifica a quien la ha realiza.

¹⁵ Nótese que todas estas definiciones apuntan a la finalidad jurídica de la firma, tal como fueran descritas en los apartados anteriores.

2º Presunción de autoría o atribución: esta surge de relacionar un determinado trazo representativo de una persona a los documentos que la contengan, por ello, si un documento determinado posee una firma se presupone que el mismo ha emanado del firmante.¹⁶

3º Conformidad con el texto que la antecede: al encontrarse la firma al final del texto hace presumir, también admitiendo prueba en contrario la conformidad del firmante con el texto anterior a la firma en sí, aunque en algunos casos por falta de espacio se pueda firmar en forma marginal, para reconocer un texto a foja completa.

4º Presunción de integridad del texto que avala: al presumirse la conformidad, se presume asimismo la integridad del texto que conforma, el mismo sin enmiendas ni raspaduras o añadidos, ya que la presunción legal alcanza al contenido completo del documento firmado y que se presume completo y conocido por el firmante, quien a través del trazo otorga su conformidad.

14. Modo en que puede ser subsanado la falta de firma autógrafa en un contrato electrónico.

¹⁶ “iuris tantum”

No sólo la firma autógrafa es capaz de satisfacer las funciones descritas precedentemente, sino que existen a la fecha otros procesos capaces de cumplir en forma integral esas funciones sin necesidad de que el “firmante” estampe su rúbrica personal y manuscrita en el documento, cosa que, además, resulta imposible si hablamos de un documento electrónico.

Este hecho, revolucionario para muchos, es posible porque existen cientos de técnicas de identificación de personas que pueden aplicarse o adjuntarse a un documento electrónico, cumpliendo así las funciones antes referidas, y aún de adaptarse a las definiciones presentadas, aun cuando no todas resultan viables en términos económicos.¹⁷

17 A efectos meramente explicativos las podemos dividir en: 1.- Firmas no autógrafas electrónicas: Son aquellas que a través de la utilización de procesos electrónicos permiten la identificación positiva del emisor de un documento y aseguran su integridad y conformidad. Dentro de este gran grupo o género podemos contar a la firma digital, a las firmas digitales sobre receptores vírgenes o aún a un simple escaneo facsimilar de una firma ológrafa. 2.- Firmas no autógrafas no electrónicas: Son aquellos procesos químicos o electroquímicos, o bien electromagnéticos o cualquier otro medio no electrónico que permita una identificación positiva del emisor de un documento o bien del que ingrese a un ámbito determinado. Dentro de este grupo podemos incluir la firma por secuencia de ADN, los identificadores electromagnéticos (como el caso de las alarmas activadas por imanes), los identificadores por radio frecuencia (RFID), los lectores ópticos de señales láser, etcétera. 3.- Firmas no autógrafas mixtas: son todos aquellos procesos que utilizan la electrónica como medio pero para la identificación del firmante dependen de parámetros de otra especie, ya sean estos

En este sentido cabe resaltar que en cada momento, y cada paso que damos usando una computadora estamos dejando una “huella digital” un fragmento de información que puede ser suficiente para vincular nuestro actuar con los contenidos guardados electrónicamente. Muchas veces esto ocurre sin darnos cuenta, y aun cuando pensamos que estamos precisamente “borrando” tales contenidos (como es el caso de “borrar” archivos, los cuales no son “realmente eliminados” sino “marcados como espacio disponible”, por lo que el archivo permanece en el computador, hasta que es efectivamente reescrito por otro, proceso que puede demorar meses, o hasta años). Estas características de los sistemas informáticos están generando una rama nueva de estudios forenses, el estudio de la “Evidencia Digital”, los que acapararon la atención de la Prensa con el caso “USA vs. Microsoft” en el año 1999, y que en la actualidad están ayudando a las policías del mundo a desarticular redes pornografía infantil en Internet.

15. Firma electrónica: Análisis somero de ciertos aspectos técnicos indispensables de tener presente.

mecánicos, físicos o biológicos. En este grupo podemos incluir por ejemplo, a los métodos biométricos, a los escáneres de huellas dactilares, a los lectores de iris, etc.

La Ley chilena define **firma electrónica** como “cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor”¹⁸. En México, por **Firma Electrónica** se debe entender “Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio”.

16. Acerca de la firma electrónica avanzada.

En Chile, la firma electrónica avanzada requiere de una comprobación previa de identidad del solicitante, hecho que debe ser verificado por el prestador de servicios, y debe ser creada utilizando medios seguros, lo que le atribuye la función de no repudio.

La letra g) del artículo 2 de la Ley 19.799, se define firma electrónica, y firma electrónica avanzada, del modo que sigue:

¹⁸ Letra f) del artículo 2 de Ley 19.799

Firma electrónica avanzada, 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***”.

El Código Comercio Mexicano ha definido, también, la **firma Electrónica Avanzada o Fiable**, pero del modo que sigue: “Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica”.¹⁹

En Chile, la fiabilidad de una firma electrónica aparece por los prestadores acreditados para certificar firmas electrónicas²⁰, los que están especialmente tratados en el título III de la mencionada

19 Los requisitos, no copulativos, son los siguientes: I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante; II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante; III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

20 Artículo 2, c) Certificador o Prestador de Servicios de Certificación: entidad prestadora de servicios de certificación de firmas electrónicas;

Ley, titulada “**DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN**”; los que son – de conformidad al artículo 11- 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*”.

Las obligaciones del prestador de servicios de certificación de firma electrónica, en lo atinente, consiste en “**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**”.

En caso de incumplimiento de esta obligación, así como de las demás impuestas en el artículo 12 de la ley 19.799, 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. Ccorrespondiéndole a ellos demostrar que actuaron

con la debida diligencia; es decir, se invierte el peso de la prueba consagrado en el artículo 1698 del Código Civil, puesto que comprobado el hecho que, producto del certificado de firmas electrónicas por ellos acreditados, se presumirá su responsabilidad. Luego, el artículo 14²¹ de la Ley 19.799 es una excepción al sistema de responsabilidad subjetiva que consagra nuestro Código Civil, dado que supone – por el contrario- una responsabilidad objetiva.

Sin perjuicio de lo anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido

²¹ 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 aquéllos 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.

o fraudulento de un certificado de firma electrónica; la que podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero, quedando - el proveedor de servicios de certificación - eximido de responsabilidad por los daños y perjuicios causados, por el uso que exceda de los límites ahí indicados.

El Código de Comercio Mexicano también contempla los prestadores de servicio de certificación, definiéndolos en su artículo 89; “Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.”

A continuación les dedica el Capítulo III “De los prestadores de Servicios de Certificación”, artículos 100 al 113, en una exhaustiva enumeración de personas o instituciones idóneas para ofrecer los servicios de certificación, forma de constituir el objeto social, requisitos a cumplir, forma de solicitar la acreditación, atribuciones, obligaciones, y otros aspectos, que en el caso de la legislación Chilena, quedaron regulados en el Reglamento de la Ley 19.799, publicado en el D.O. el 17 de agosto de 2002.

En su artículo 100 establece quienes pueden ser Prestadores de Servicios de Certificación:

- I.** Los notarios públicos y corredores públicos;
- II.** Las personas morales de carácter privado, y
- III.** Las instituciones públicas, conforme a las leyes que les son aplicables.

Es interesante notar que el legislador mexicano señala que “La facultad de expedir Certificados no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.” Zanjando de una vez las posibles dudas que pudieran haber existido, al ser posible que algunos ministros de fe cumplan una función dual.

En cuanto a los derechos y obligaciones de los usuarios de firmas electrónicas, la situación difiere entre ambas legislaciones.

La ley mexicana establece obligaciones para el firmante en su artículo 99.

Estas obligaciones son las siguientes:

I. Cumplir las obligaciones derivadas del uso de la Firma Electrónica;

II. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma;

III. Cuando se emplee un Certificado en relación con una Firma Electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el Certificado, con su vigencia, o que hayan sido consignadas en el mismo, son exactas. El Firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en el presente artículo, y

IV. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia.

Situación que contrasta con la legislación Chilena, que solo menciona en su 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.” El incumplimiento de las obligaciones contenidas en este artículo trae consigo la inhabilidad del certificado para seguir produciendo efectos jurídicos, en concordancia con el artículo 16 no.2 de la mencionada Ley 19.799, más dista de las drásticas sanciones y presunciones de responsabilidad que impone su contraparte mexicana. En consecuencia, la responsabilidad civil (y penal si es procedente) en caso de uso no autorizado de la firma electrónica debe regirse según las reglas generales.

17. Valor probatorio de los documentos electrónicos, en Chile.

Según dispone la misma ley, la firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio que los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse

mediante **firma electrónica avanzada**²²; de este modo, nuestro legislador comparte con la legislación mexicana **la equivalencia funcional de la Firma Electrónica en relación con la firma autógrafa**, que resulta más explícito – en esta materia- con nuestro principio de **equivalencia del soporte electrónico al soporte de papel**.

El artículo 5° establece las reglas para que los documentos electrónicos puedan ser usados como medio de prueba en juicio:

1.- Los documentos electrónicos que tengan la calidad de instrumento público, harán plena prueba de acuerdo con las reglas generales; y

2.- Los que posean la calidad de instrumento privado, en cuanto hayan sido suscritos mediante firma electrónica avanzada, harán plena prueba de acuerdo con las reglas generales. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales.

Nuestro Código de Procedimiento Civil, aplicable en todos aquellos asuntos civiles y comerciales, subsidiariamente en las cuestiones laborales, consagra el sistema de prueba legal tasada,

²² Artículo 4 de la Ley 19.799.

por ello, no es irrelevante la circunstancia que los documentos electrónicos que contengan la firma electrónica avanzada, sean equiparados a los documentos electrónicos que tengan la calidad de instrumento público, puesto ambos producirán plena prueba.

Los que no estén suscritos mediante firma electrónica avanzada, tendrán el valor de instrumentos privados; y, para que produzcan plena prueba en juicio, deberán ser acompañados en alguna de las formas establecidas en el artículo 346 del Código referido.

En materia penal, se ha consagrado el sistema de Libertad de Prueba, o de libre convicción, según el cual por cualquier medio de prueba se puede probar el hecho punible y la participación del imputado en éste, siempre que produzcan en los sentenciadores, la convicción, más allá de toda duda razonable, que ha acaecido el hecho ilícito, y que al acusado la ha cabido participación en él, en calidad de autor, cómplice o encubridor. Y, en tal sentido, los documentos electrónicos, incorporados en el juicio en forma legal, podrán ser valorados libremente por los jueces.

18. Valor probatorio de los documentos electrónicos, en México.

La legislación mexicana, al definir la firma electrónica, termina señalando que es admisible como prueba en juicio, consecuencia necesaria de la circunstancia que le otorga los mismos efectos jurídicos de la firma autógrafa a la firma electrónica.

Es decir, se le otorgará valor probatorio, en la medida que pueda vincularse al signatario con el “mensaje de datos” y su autoría.

En tal sentido, el referido código establece las bases que permitan presumir que un mensaje de datos con un determinado emisor, y ello ocurre, si ha sido enviado:

I. Por el propio Emisor;

II. Usando medios de identificación, tales como claves o contraseñas del Emisor o por alguna persona facultada para actuar en nombre del Emisor respecto a ese Mensaje de Datos, o

III. Por un Sistema de Información programado por el Emisor o en su nombre para que opere automáticamente.

Además, a continuación, regla en forma detallada los casos en que se pueda presumir **que un Mensaje de Datos ha sido**

enviado por el Emisor y, por lo tanto, el Destinatario o la Parte que Confía, en su caso, podrá actuar en consecuencia:

I. Haya aplicado en forma adecuada el procedimiento acordado previamente con el Emisor, con el fin de establecer que el Mensaje de Datos provenía efectivamente de éste, o

II. El Mensaje de Datos que reciba el Destinatario o la Parte que Confía, resulte de los actos de un Intermediario que le haya dado acceso a algún método utilizado por el Emisor para identificar un Mensaje de Datos como propio.

III. A partir del momento en que el Destinatario o la Parte que Confía, haya sido informado por el Emisor de que el Mensaje de Datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia; y,

IV. A partir del momento en que el Destinatario o la Parte que Confía, tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el Mensaje de Datos no provenía del Emisor. Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del Emisor, se presumirá que se actuó con la debida diligencia si el método que usó el

Destinatario o la Parte que Confía cumple con los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas.

19. De la fiabilidad de la información contenida en el documento electrónico, en relación con la información documentada en medios no electrónicos.

El **principio de equivalencia del soporte electrónico al soporte de papel**, es indispensable para crear verdadera seguridad jurídica en el uso habitual de los medios informáticos y telemáticos para la realización de operaciones comerciales.

El Código de Comercio Mexicano, como ya se señaló, se refiere a ella como **“equivalencia funcional de la información contenida en el mensaje de datos, en relación con la información documentada en medios no electrónicos y de la firma electrónica en relación con la firma autógrafa.”**

Estos principios sólo han podido ser consagrados, gracias a que la ciencia tecnológica permite dar fe no sólo de las fechas en

que se confeccionan los documentos, sino que también las modificaciones que se hagan a ésta.²³

El modo de resolver la cuestión planteada parece ser simple, si el “*documento electrónico*” (o el “mensaje de datos”) cumple iguales funciones prácticas que los documentos en papel, debería otorgarse a ambos igual valor jurídico.

Al respecto, y con relación a una de las fuentes de inspiración tanto de la ley 19.799 como del Código de Comercio Mexicano, consideramos apropiado incluir el siguiente extracto de la “Guía para la incorporación al derecho interno de la Ley Modelo de la UNCITRAL sobre Comercio Electrónico”.

“... la Ley Modelo sigue un nuevo criterio, denominado a veces "criterio del equivalente funcional", basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico. Por ejemplo, ese documento de papel cumple funciones como las siguientes: proporcionar un documento legible para todos; asegurar la

²³ Ver punto 14 de este capítulo.

inalterabilidad de un documento a lo largo del tiempo; permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito; permitir la autenticación de los datos consignados suscribiéndolos con una firma; y proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales. Cabe señalar que, respecto de todas esas funciones, la documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, mucha mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos, con tal que se observen ciertos requisitos técnicos y jurídicos..."

Esta equivalencia funcional permite la solución de uno de los principales problemas que obstaban a la valoración del documento electrónico como documento privado.

En nuestra legislación, el referido principio, aparece consagrada en la forma ya indicada, y concretizada en el inciso primero del artículo 3º, de la Ley N° 19.799, dispone:

“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 reputan 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.”

Sin embargo, la Ley mencionada no se ocupa de aspectos tales como quien ha enviado el documento electrónico, momento en que es expedido y el de su recepción, lugar de expedición, detalles que no son irrelevantes, puesto que son los que determinarán, ante cualquier dificultad, la competencia de los tribunales y la ley que se deberá aplicar.

Por su parte, el Código del Comercio Mexicano, sí se ocupa en detalle de aspectos tales como determinar el lugar y momento de expedición y recepción de un mensaje de datos²⁴; reglando,

²⁴ Artículos 91, 91 bis y 94: Artículo 91.- Salvo pacto en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará como sigue:

I. Si el Destinatario ha designado un Sistema de Información para la recepción de Mensajes de Datos, ésta tendrá lugar en el momento en que ingrese en dicho Sistema de Información;

II. De enviarse el Mensaje de Datos a un Sistema de Información del Destinatario que no sea el Sistema de Información designado, o de no haber un Sistema de Información designado, en el momento en que el Destinatario recupere el Mensaje de Datos, o

III. Si el Destinatario no ha designado un Sistema de Información, la recepción tendrá lugar cuando el Mensaje de Datos ingrese a un Sistema de Información del Destinatario.

incluso, el modo de acusar recibo de un mensaje.²⁵ Pero, en lo que ahora nos ocupa, el principio de equivalencia en los documentos

Lo dispuesto en este artículo será aplicable aun cuando el Sistema de Información esté ubicado en un lugar distinto de donde se tenga por recibido el Mensaje de Datos conforme al artículo 94.

Artículo 91 bis.- Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido cuando ingrese en un Sistema de Información que no esté bajo el control del Emisor o del Intermediario.

Artículo 94.- Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido en el lugar donde el Emisor tenga su establecimiento y por recibido en el lugar donde el Destinatario tenga el suyo. Para los fines del presente artículo:

I. Si el Emisor 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, y

II. Si el Emisor o el Destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

25 Artículo 92.- En lo referente a acuse de recibo de Mensajes de Datos, se estará a lo siguiente:

I. Si al enviar o antes de enviar un Mensaje de Datos, el Emisor solicita o acuerda con el Destinatario que se acuse recibo del Mensaje de Datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

- a) Toda comunicación del Destinatario, automatizada o no, o
- b) Todo acto del Destinatario, que baste para indicar al Emisor que se ha recibido el Mensaje de Datos.

II. Cuando el Emisor haya indicado que los efectos del Mensaje de Datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el Mensaje de Datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo en el plazo fijado por el Emisor o dentro de un plazo razonable atendiendo a la naturaleza del negocio, a partir del momento del envío del Mensaje de Datos;

III. Cuando el Emisor haya solicitado o acordado con el Destinatario que se acuse recibo del Mensaje de Datos, independientemente de la forma o método determinado para efectuarlo, salvo que:

- a) El Emisor no haya indicado expresamente que los efectos del Mensaje de Datos estén condicionados a la recepción del acuse de recibo, y

electrónicos, aparece consagrado, siempre que – según señala el artículo 93- la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, y, según el inciso final del artículo 93 bis, *“se considerará que el contenido de un Mensaje de Datos es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso”*.²⁶

b) No se haya recibido el acuse de recibo en el plazo solicitado o acordado o, en su defecto, dentro de un plazo razonable atendiendo a la naturaleza del negocio.

El Emisor podrá dar aviso al Destinatario de que no ha recibido el acuse de recibo solicitado o acordado y fijar un nuevo plazo razonable para su recepción, contado a partir del momento de este aviso. Cuando el Emisor reciba acuse de recibo del Destinatario, se presumirá que éste ha recibido el Mensaje de Datos correspondiente;

IV. Cuando en el acuse de recibo se indique que el Mensaje de Datos recibido cumple con los requisitos técnicos convenidos o establecidos en ley, se presumirá que ello es así.

26 Al caso son aplicables los artículos 93, 93 bis y 95, que son del siguiente tenor:

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

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de Mensajes de Datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso

En nuestra legislación, la circunstancia que un determinado documento electrónico sea íntegro, también aparece asegurado si ha sido suscrito mediante **Firma electrónica avanzada**, puesto que de ese modo se podrá detectar “*cualquier modificación*,

el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo 93 bis.- Sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos:

I. Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma, y

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

Para efectos de este artículo, se considerará que el contenido de un Mensaje de Datos es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 95.- Conforme al artículo 90, siempre que se entienda que el Mensaje de Datos proviene del Emisor, o que el Destinatario tenga derecho a actuar con arreglo a este supuesto, dicho Destinatario tendrá derecho a considerar que el Mensaje de Datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El Destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error en el Mensaje de Datos recibido.

Se presume que cada Mensaje de Datos recibido es un Mensaje de Datos diferente, salvo que el Destinatario sepa, o debiera saber, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que el nuevo Mensaje de Datos era un duplicado

verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.”

20. Algunas consideraciones acerca de la Integridad en el Documento Electrónico.

En materia de comunicaciones electrónicas, el aseguramiento de la integridad del documento es una función entregada a la criptografía. Del griego *kryptos* (ocultar) y *grafos* (escribir), literalmente escritura oculta, la criptografía es el "arte de escribir con clave secreta o de un modo enigmático"²⁷. En otras palabras es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos. La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etcétera), y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser; y por último impedir que el contenido del mensaje enviado (habitualmente denominado criptograma) sea modificado en su tránsito.

²⁷ Definición del Diccionario de la Real Academia Española

Otro método utilizado para ocultar el contenido de un mensaje es ocultar el propio mensaje en un canal de información, pero en puridad, esta técnica no se considera criptografía, sino esteganografía. Por ejemplo, mediante la esteganografía se puede ocultar un mensaje en un canal de sonido, una imagen o incluso en reparto de los espacios en blanco usados para justificar un texto. La esteganografía no tiene porqué ser un método alternativo a la criptografía, siendo común que ambos métodos se utilicen de forma simultánea.

Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías de la información es el de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo. Para efectos explicativos exclusivamente técnicos, aquí consideramos la “firma digital” solo como una secuencia de *bits* que satisfacen uno de varios estándares. Es la generación de estos *bits* y su interpretación a posteriori lo que distingue esta secuencia de bits de cualquier otra. Las técnicas de cifrado o protocolos de criptografía utilizados para este proceso son los elementos claves

para otorgar y garantizar la integridad del mensaje de datos o contenido del documento electrónico.

Existen dos grandes grupos de *técnicas de cifrado*: los algoritmos²⁸ que utilizan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado* y los que utilizan una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Los primeros se denominan **cifras simétricas** o de **clave simétrica** y son la base de los algoritmos de cifrado clásico. Los segundos se denominan **cifras asimétricas**, de **clave asimétrica** o de **clave pública** y **clave privada** y forman en núcleo de las técnicas de cifrado modernas. En éste método se usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje. Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin

²⁸ Un algoritmo es un conjunto finito de instrucciones o pasos que sirven para ejecutar una tarea o resolver un problema.

de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario.

Otra técnica de la que es posible valerse para certificar la integridad del contenido del mensaje de datos (o texto a encriptar) es incluir un “*hash*”, o “*resumen de reducción criptográfica*”. Este consiste en un número (generalmente de 128 bits) que funge como “huella digital” del contenido del archivo. Este “hash” se genera basándose en los contenidos del mensaje de datos, más una función de encriptado que genera un resumen de características únicas al documento de que se trate. El “hash” en consecuencia puede ser recalculado para confirmar si un mensaje de texto ha sido alterado o no, es “repetible” en el sentido que usando el mismo algoritmo y sobre el mismo mensaje de texto, el mismo “hash” será producido. La variación de tan solo un carácter (como por ejemplo; cambiar una coma por un punto) generará un “hash” totalmente distinto, indicando que el mensaje ha sido adulterado

en tránsito. Además el “hash” funciona en un solo sentido, por lo que no es posible descubrir ya sea, el contenido del mensaje, o la clave usada para crear el “hash” mirando solo el número resultante.

Conclusiones

a) Conforme aumenta el uso de Internet para celebrar contratos, van surgiendo controversias y conflictos, mismos que en muchas ocasiones requieren de una intervención judicial para llegar a un acuerdo entre las partes.

Generalmente se trata de los mismos problemas que se presentan en el comercio tradicional, pero ahora aplicados a situaciones relacionadas con el ciberespacio, donde la comunicación se realiza por medio de mensajes electrónicos.

Hoy en día muchos dudan o ignoran sobre la validez de utilizar documentos electrónicos como medio de prueba.

Probablemente la mayoría de las legislaciones establecen restricciones estrictas o taxativas a los medios de prueba, y, considerando el carácter novedoso y reciente de las tecnologías de la informática y el comercio electrónico, obviamente no contemplan entre sus medios de prueba a los documentos electrónicos.

b) El problema se acrecienta al recordar el retraso tecnológico en el Poder Judicial de muchos países. Así, se dificulta enormemente la utilización de los documentos electrónicos como

medio de prueba, debido a que los jueces no tienen, en la mayoría de las ocasiones, una mínima preparación técnica para operar computadores²⁹ y, consiguientemente, trabajar con este tipo de documentos; reconociendo el valor probatorio de este tipo de documentos, de manera de garantizar la posibilidad de exigir el cumplimiento, por la vía judicial.

Debemos considerar que en la valorización de las pruebas que realizan los jueces, ellos recurren necesariamente a apreciaciones y opiniones que, hasta cierto punto, pudieran calificarse como subjetivas, siempre y cuando lo hagan basándose en la razón y su experiencia. Así, entrarán a analizar ciertos elementos de la prueba, como su integridad, inalterabilidad, veracidad y exactitud.

Y, como ya observamos, gracias a los avances tecnológicos es innegable que los documentos electrónicos pueden llegar a cumplir de hecho con los requisitos de las pruebas que analizarán los jueces. E incluso más, las superan en integridad e inalterabilidad. Es por eso que en esa valorización "subjetiva" el juez deberá considerar estas características de los documentos electrónicos.

²⁹ En la actualidad la Academia Judicial Chilena ofrece cursos de capacitación en el uso de computadoras y paquetes de programas.

c) El impacto que está teniendo el Comercio Electrónico en el funcionamiento de la sociedad hace indispensable el adecuado reconocimiento legal de los acuerdos y demás contratos celebrados electrónicamente, de manera que sea posible utilizar los documentos digitales, o aquellos que no constan en el "papel tradicional", como medio probatorio, perfectamente válido, en cualquier procedimiento judicial.

En muchas ocasiones, con meras inserciones en la legislación probatoria bastará para incluir y reconocer legalmente a los documentos electrónicos como medio de prueba.

Estas modificaciones deberán ser flexibles para adaptarse a la evolución de los mercados electrónicos, de manera que éstos en todo momento puedan considerarse como vías seguras de contratación, y proteger la obligatoriedad jurídica de los acuerdos alcanzados en el ciberespacio.

Sin embargo, en la realidad muchas veces esta regulación no será suficiente, ya que las personas que van a aplicar la ley necesariamente deben conocer los límites y capacidades de las tecnologías de la informática, para lograr una adecuada valorización de los documentos electrónicos. Asimismo, será

indispensable contar con la infraestructura física de herramientas, como computadores actualizados, que permitan recibir las pruebas que consten en documentos electrónicos.

d) Si bien no puede negarse validez a los documentos electrónicos por no estar expresados en manera tradicional de soporte papel, sin perjuicio que se admite los documentos electrónicos como prueba en juicio de pruebas electrónicas, y que incluso, en nuestra legislación se señala el peso de la prueba, según si la firma es o no “avanzada”, no ha sido debidamente tratado el caso en que impugnen de falsedad o repudio de la firma por el titular.

Tales incidentes deberían, pues, ser solucionados de la forma establecida en el Código de Procedimiento Civil, pudiendo pedirse su cotejo, y nombrar peritos revisores, siempre que se niegue por la parte a quien perjudique o se ponga en duda la autenticidad de un documento privado o la de cualquier documento público que carezca de matriz, cual sería el caso de un documento electrónico suscrito con firma electrónica avanzada.

Incluso, los medios probatorios admitidos en el incidente sobre autenticidad de un instrumento no se limitarán al cotejo,

sino que también, aquellos que las leyes autorizan para la prueba del fraude, referencia que debe entenderse hecha al Código Procesal Penal, la que consagra la libertad de la prueba o de libre convicción. En la apreciación de la prueba, el Tribunal se sujetará a las reglas de la apreciación comparativa de los medios de prueba.

e) El único problema que puede representar la desavenencia lingüística existente entre la ley chilena y la mexicana, en relación al documento electrónico y mensaje de datos, en la mayoría de las legislaciones internacionales al que se concede equivalencia es al documento electrónico; y, al momento de medir la compatibilidad internacional, es la ley y no los medios técnicos, la que presenta algunas diferencias, que pueden quedar salvadas por la definición, pero en algunos casos podría generar inconvenientes en la redacción de los convenios particulares entre usuarios si el punto no es debidamente aclarado en los textos mismos de los instrumentos de contratación, ya que no debemos olvidar que algunas leyes manejan los conceptos de Mensaje de Datos y Documento Electrónico como elementos distintos, de los cuales el segundo es género de la especie del primero, ya que no todo

documento electrónico tiene por finalidad expresa ser transmitido como Mensaje de Datos.

f) Existen infinidad de normas penales, de procedimiento penal, civil y comercial que no son claramente adaptables a las firmas electrónicas y es justamente allí donde de seguro han de producirse los fallos de la ley en particular.

Veamos algunos ejemplos: Ambas legislaciones establecen penas a quienes falsifiquen documentos, sean éstos públicos o privados y dentro de algunas modalidades relata expresamente la utilización de firma falsa.³⁰ ¿Qué pasa pues si el documento que se falsifica es electrónico?. ¿Qué ocurre si se abusa de una firma electrónica?

En estricto rigor, como en materia penal gobierna expresamente el principio de *nullum crime, nulla poena sine lege*, debo concluir que la falsificación de un documento electrónico no es a la fecha delito punible y la seguridad jurídica que pretende otorgar la ley por medio de la equivalencia funcional es un gigante con pies de barro, ya que no se otorga protección jurídica ante los

³⁰ Código Penal Chileno, artículo 197 y Código Penal Federal, artículos 243 y 244.

posibles casos de fraude que tan comunes son en nuestros días por medio de estos nuevos elementos tecnológicos.

g) No obstante lo anterior, creemos que nuestro país se encuentra en inmejorable situación en la región para liderar el desarrollo del comercio electrónico, tanto a nivel privado como a nivel estatal, destacándose en este último punto, la decidida actitud del actual gobierno de abrazar las nuevas tecnologías y procurar darles cabida en la medida de lo posible. En su Instructivo Sobre *“Política Nacional para la Participación Activa de los Organismos Públicos en el Uso de Internet”*, de fecha 9 de abril de 2001, el Presidente de la República señala que en el plan de modernización del Estado se han destacado como prioridades el desarrollo y la masificación de nuevas tecnologías de información. En ellas se reconoce a Internet como la principal oportunidad de crecimiento y desarrollo de los países dentro del nuevo milenio, representado nuevas expectativas dentro del marco de la denominada nueva economía.

Continúa señalando que Chile posee ventajas comparativas con respecto a otros países de la región, en cantidad de computadores y porcentaje de usuarios de Internet, y que es

necesario transmitir a los ciudadanos una clara señal de confianza y conveniencia en el uso de las nuevas tecnologías.

Estas palabras y este mensaje se han concretizado en una renovación de las formas de acceso a la información y servicios en línea que actualmente ofrecen oficinas públicas como el Servicio de Impuestos Internos o el Registro Civil e Identificación, donde hoy es posible pagar impuestos en línea, obtener facturas electrónicas, requerir extractos de filiación y certificados de antecedentes, entre otros.

En el ámbito privado, desde hace años que es posible realizar transferencias bancarias, contratar depósitos, realizar pagos de servicios, consultar saldos en línea, etcétera.

Desde el advenimiento del World Wide Web, es posible comprar cualquier clase de bienes muebles en cualquier parte del mundo, y recibirlos en nuestra puerta, sin haber siquiera dejado nuestro escritorio.

El reconocimiento de facto y la confianza de que goza el documento electrónico entre quienes lo usan a diario, lentamente se abre camino hacia el común de la población, en donde

esperamos se encuentre respaldado además, de una jurisprudencia uniforme por parte de nuestra Judicatura.

Bibliografía:

BETTENDORF, Jorg, “Documentos procesados electrónicamente”

CARRASCOSA LOPEZ, Valentín, “El derecho de la prueba y la informática. Informática y Derecho.”

CARRASCOSA LOPEZ, V. y otros, “La contratación Informática, el nuevo horizonte contractual.”

CAVAZOS Edgard, & MORIN Gavino, “Cyberspace and the law.”

COUTURE Eduardo, “El concepto de Fe publica.”

COUTURE Eduardo, “Fundamentos del derecho procesal civil”

GAETE GONZALEZ Eugenio, “La reproducción facsimilar. Problemas jurídicos que plantea.”

GAETE GONZALEZ Eugenio, “Documento Informático y seguridad jurídica.”

LEON HURTADO Avelino, “La voluntad y la capacidad en los actos jurídicos”

LOPEZ SANTA MARIA, Jorge, “Problemas actuales en el derecho de los contratos”

MARONDA FRUTOS Juan Luis, y TENA FRANCO Maria Isabel, “La informática jurídica y el derecho de la información.”

NORMA Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales- Requisitos que deben observarse para la conservación de mensajes de datos.

RIOSECO ENRIQUEZ Emilio, “La prueba ante la jurisprudencia.
Derecho Civil y Derecho Procesal Civil”

ORMAZABAL SANCHEZ, Guillermo, “Valor probatorio del documento
signado en forma digital”

UNCITRAL, “Ley tipo sobre comercio electrónico”

VIVANT y otros, “Derecho de la Informática”

VALOR PROBATORIO DE LOS DOCUMENTOS ELECTRÓNICOS.....	1
Introducción	1
1er. Capitulo: De la Internet y el Documento Electrónico.....	11
1. Que es Internet.	11
2. Documento Electrónico.	12
3. De los contratos, en general, a la especificación de los contratos electrónicos.	16
4. Acerca de la prueba de los contratos electrónicos.	19
5. Principios que informan las legislaciones chilenas y Mexicana en relación a los documentos electrónicos.	20
6.- Definición legal de Documento electrónico.	23
7. Valor probatorio de los documentos electrónicos.....	24
2do. Capitulo: Problemática Jurídica Del Valor Probatorio De Los Documentos Electrónicos.....	29
8.- Planteamiento del problema.	29
9.-Análisis del problema planteado, nociones preliminares de la firma:	30
10. Categorías de firmas.	30
La firma se puede separar en dos grandes grupos o categorías:	31
11. Referencias históricas:	31
12. Definición de firma:	32
13. Funciones de la firma:.....	33
14. Modo en que puede ser subsanado la falta de firma autógrafa en un contrato electrónico.	34
15. Firma electrónica: Análisis somero de ciertos aspectos técnicos indispensables de tener presente.	36
16. Acerca de la firma electrónica avanzada.....	37
17. Valor probatorio de los documentos electrónicos, en Chile.	44
18. Valor probatorio de los documentos electrónicos, en México.....	46
19. De la fiabilidad de la información contenida en el documento electrónico, en relación con la información documentada en medios no electrónicos.	49
20. Algunas consideraciones acerca de la Integridad en el Documento Electrónico.	56
Conclusiones	61
Bibliografía:	70