UNIVERSIDAD CATÓLICA "ANDRÉS BELLO"
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
ÁREA DE DERECHO
ESPECILIDAD EN DERECHO PROCESAL

VALOR PROBATORIO DEL MENSAJE DE DATOS Y LA FIRMA ELECTRONICA

Trabajo Especial de Grado, presentado como requisito parcial para optar al Grado de Especialista, en Derecho Procesal.

Autora: Abog. Yraima Agularte

Asesor: Msc. Andrés Octavio Méndez Carvallo

Caracas, Mayo 2004

ÍNDICE

A mis padres quienes estuvieron conmigo al comenzar este trabajo y hoy se encuentran ausentes, desde el cielo, se que me apoyan.
A mis hijos Yraima y José Miguel, amores de mi vida.
A Sol Maria, por su apoyo y comprensión en todo momento.

"UNIVERSIDAD CATÓLICA "ANDRÉS BELLO"
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
ÁREA DE DERECHO
ESPECILIDAD EN DERECHO PROCESAL

VALOR PROBATORIO DEL MENSAJE DE DATOS Y LA FIRMA ELECTRONICA

Autora: Abog. Yraima Agularte
Asesor: Msc. Andrés Octavio Méndez Carvallo
Fecha: Mayo de 2004

RESUMEN

El derecho a la prueba está íntimamente ligado con el derecho a la defensa y conlleva a determinar cuando un proceso se ha realizado tomando en cuenta todas las garantías.
Un contrato realizado por vía electrónica adquiere relevancia jurídica fundamental, la determinación de la competencia, la jurisdicción, el momento determinante de su formación, la desmaterialización de los documentos y la fijación y problemática de la prueba que determine el consentimiento, lugar, contenido y partes del contrato, debido a que la transferencia electrónica de datos permite intercambiar mensajes normalizados en lugar de documentos escritos.
Al hablar de valor probatorio del mensaje de datos y la firma electrónica, se está haciendo referencia a la adecuación que deben tener las pruebas con el tema u objeto del litigio. El derecho a la prueba va unido al derecho a la defensa y conlleva la determinación si un derecho se ha realizado con todas las garantías
Lo que interesa y da validez a las pruebas empleadas es la relación que las pruebas guardan con lo que constituye el tema desidendi para el tribunal y expresa la capacidad de los medios utilizados para formar la definitiva convicción del Juez. Una prueba aportada por medio de dispositivos electrónicos debe ser valorada por el Juez y en caso de negarse su admisión o de no valorarse se puede intentar un amparo.

INTRODUCCIÓN

Las redes abiertas como Internet revisten cada vez mayor importancia para la comunicación mundial. Esas redes permiten una comunicación interactiva entre interlocutores que no necesariamente han entablado previamente relación alguna. Además, ofrecen nuevas posibilidades empresariales, creando herramientas que mejoran la productividad y reducen los costos, así como nuevas formas de llegar al cliente. Las redes están siendo utilizadas por empresas que desean aprovechar los nuevos tipos de actividad y nuevas formas de trabajo, como el tele-trabajo y los entornos virtuales compartidos.

También las administraciones públicas las utilizan en su gestión interna y en su interacción con empresas y ciudadanos. El comercio electrónico brinda al país una excelente oportunidad para avanzar en su integración económica con las naciones del resto del mundo.

Para aprovechar todas estas posibilidades es necesario disponer de un entorno seguro en relación con la autenticación digital. En la práctica existen diversos métodos para firmar documentos digitalmemente, que van desde algunos muy sencillos por ejemplo, insertar la imagen escaneada de una firma manuscrita en un documento creado con un procesador de texto que no permiten otorgarle validez jurídica a la firma, a otros muy avanzados, por

ejemplo la firma digital que utiliza la "criptografía" de clave pública", que sí lo permiten.

Se entiende por criptografía la técnica que permite modificar un mensaje original mediante una o varias claves, de forma que quede totalmente ilegible ante cualquier persona, excepto aquella que tenga la clave adecuada para desencriptar. Esto permite enviar información a través de la red con seguridad de que no podrá ser vista por ninguna persona ajena al mensaje. La criptografía garantiza la confidencialidad de la comunicación enviada a través de la red, es decir, la no-vulnerabilidad de la información ya que, de interceptarse los mensajes por terceros, éstos no serán comprendidos pues lo escrito resultaría indescifrable.

La computadora, para procesar una información, la transforma en impulsos electrónicos que lee como pares de 0 y 1. A través del proceso de encriptación, los pares de ceros y unos que forman el mensaje a enviar son mezclados y desorganizados para que los datos no resulten legibles. Quien desee entender el mensaje, deberá poseer una clave que permita reordenar [9]la estructura inicial. Si el procedimiento para encriptar un mensaje y luego desencriptarlo está compuesto por una única fórmula, entonces concluiremos

que la clave utilizada para tales funciones es la misma y por tanto estaremos ante una "clave simétrica".

Para tener validez jurídica, las firmas digitales deben permitir verificar tanto la identidad del autor de los datos (*autenticación de autoría*), como comprobar que dichos datos no han sufrido alteración desde que fueron firmados (*integridad*).

El documento digital, es simplemente una secuencia informática de bits (unos y ceros) que puede representar cualquier tipo de información. Esta representación de la información sobre la base de dígitos implica en el ámbito informático una representación binaria, es decir por medio de unos y ceros.

Todo tipo de información es apta para ser representada digitalmente: Mediante el escaneo, la imagen de una fotografía o la imagen de un documento en soporte papel; mediante un procesador de palabras, la información escrita; mediante una plaqueta digitalizadora, la voz, la música y el video; mediante hojas de cálculo, la información numérica y financiera; y

mediante bases de datos, la información estadística y diversos bancos de información.

Toda información representada digitalmente constituye un documento digital y es susceptible de ser firmada digitalmente. Es por ello que la firma digital puede utilizarse para otorgar validez jurídica o eficacia probatoria a toda declaración de voluntad o de conocimiento, con independencia de su extensión o de su medio de almacenamiento, sin limitación alguna.

La pretensión jurídica invocada en juicio debe ser acreditada mediante las reglas dadas por el derecho probatorio de cada país, ya que de ello depende la efectiva titularidad sobre un derecho discutido o negado. Por ello, la prueba se constituye en la base fundamental del proceso y en una condición de seguridad jurídica esencial para el pronunciamiento de una sentencia justa y objetiva.

Ahora bien, el creciente empleo de las tecnologías de la información como soporte material en el cual se concretan hechos y actos jurídicos actualmente, nos ha motivado a dedicar un breve estudio sobre el documento electrónico como un medio de prueba admisible, especialmente en caso de ausencia de consagración expresa en el ordenamiento jurídico.

Ante todo, advirtamos que nos referiremos al documento electrónico en su sentido estricto, es decir, entendiéndolo como una representación material, destinada e idónea para reproducir una cierta manifestación de voluntad, materializada a través de las tecnologías de la información sobre soportes magnéticos, como un disquete, un CD-ROM, una tarjeta inteligente u otro, y que consisten en mensajes digitalizados que requieren de máquinas traductoras para ser percibidos y comprendidos por el hombre; como también, abordaremos a los documentos electrónicos en sentido amplio o documentos informáticos, caracterizados por la posibilidad de ser percibibles y legibles directamente por el hombre sin necesidad de la intervención de máquinas traductoras, como sería el caso de la boleta que emite un cajero automático o un correo electrónico impreso.

No obstante, estar adquiriendo mayor habitualidad y trascendencia en la contratación moderna y en los medios de pago, los soportes informáticos no están ajenos a importantes críticas que cuestionan no sólo su valor probatorio sino incluso su admisibilidad como medio de prueba. Las dudas que despierta parten de la estabilidad de su contenido, su originalidad y la identificación del autor por medio de la firma.

En primer lugar, la estabilidad del contenido de estos nuevos documentos aún no ha sido capaz de brindar garantías suficientes de confiabilidad al juez para que se forme convicción de los hechos, debido a que la inalterabilidad y el carácter indeleble de los elementos de registro empleados desaparece si éstos pueden ser sobrescritos o borrados.

Además, por lo general los documentos electrónicos son la transcripción de una escritura sobre papel que, con frecuencia, se destruye después de registrarse digitalmente, y además, las copias digitales son idénticas a su matriz, por eso se duda sobre su carácter original. Este último punto suele depender principalmente del grado de inalterabilidad e integridad del contenido que presente el documento.

Finalmente, las críticas a la admisibilidad del documento electrónico se dirigen contra de la validez de la firma electrónica. La firma manuscrita tradicional no es aplicable al documento electrónico; es más, hay una suerte de incompatibilidad de los medios informáticos con la exigencia de firma (por las trabas a la operabilidad y celeridad que implicaría), generándose un problema al no aceptarse métodos substitutivos de ella para comprobar la autoría de un documento e imputar responsabilidad por sus efectos.

Sin embargo, hoy existe un consenso sobre la necesidad de aceptar a la firma digital lo antes posible en las legislaciones, por ser el sustento que permitirá, por ejemplo el sano desarrollo del comercio electrónico. Por ello, en la práctica se han creado autoridades certificadoras, públicas y privadas, cuya función consiste en expedir certificados con los que se identifica a los usuarios, asignándoseles una clave pública para usarla en las comunicaciones electrónicas. El número de estas autoridades certificadoras ha crecido rápidamente.

No obstante, visto que sus actividades se basan en una tecnología nueva, cuya eficiencia tendrá que probarse mediante un uso más prolongado, sigue existiendo cierta incertidumbre sobre si las autoridades certificadoras podrán satisfacer plenamente la necesidad de seguridad en las comunicaciones electrónicas.

Además, desde un punto de vista legal, se propone la homologación de la firma digital con la firma manuscrita, eso sí, determinando el campo de aquélla, ya que hay actos jurídicos que no aconsejan su utilización. Por último, agregaremos que para lograr autenticar la firma digital se recurre principalmente a técnicas criptográficas, junto con otras complementarias como los códigos secretos o la biometría, todo lo cual será un efectivo

elemento de certeza una vez que puedan formar parte de tecnologías accesibles a la generalidad de la población, tanto en sus costos como en su utilización.

I. ORIGENES Y EVOLUCION DEL DOCUMENTO ELECTRÓNICO EN VENEZUELA.

Durante el siglo XX han surgido innumerables técnicas que han ido produciendo a su vez incontables nuevas formas de representación y transmisión del pensamiento humano. Desde la fotografía que ya existía en el siglo XIX hasta las cintas magnetofónicas, el telex, el fax, el telefax, los videos, los disquetes, los discos ópticos. Todos ellos engloban un conjunto nada homogéneo de objetos representadores de hechos con potencial relevancia jurídica, siendo los soportes informáticos los que menos atención doctrinal han suscitado por parte de los procesalistas y como apunta Álvarez llama la atención el tremendo contraste entre la masiva aplicación de los sistemas electrónicos en la contratación empresarial y la carencia de normas para regular la prueba de estas operaciones. (1997,1937).

Sostiene Sanchis (1999,24) que la posibilidad de admitir como prueba documental los modernos medios de reproducción de la información tiene una importancia creciente debido, por un lado, a la propia de la prueba documental y, por otro, al vertiginoso ritmo de progresiva sustitución de los

documentos tradicionales por estos otros soportes. Por ello la eludida falta de tratamiento tanto más llamativa.

En nuestro país se dictó el Decreto con Fuerza de Ley nº 37.148 el veintiocho (28) de febrero de 2001 sobre Mensajes de Datos y Firmas Electrónicas, cuyo ámbito de aplicación es otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y los certificados electrónicos.

Además establece dicho Decreto que será aplicable a los mensajes de datos y firmas electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los mensajes de datos y firmas electrónicas.

A. ANTECEDENTES.

Para llegar a un concepto nuevo y más amplio de documento debemos examinar los posibles obstáculos que existen en torno a dicho concepto.
En primer lugar, encontramos la barrera legal y de otro lado la falta de fidelidad y perdurabilidad que se les atribuye a los nuevos documentos.

En cuanto a la barrera legal sostiene Sanchis que según el derecho positivo, resulta innegable que de nuestras leyes procesales se desprende inequívocamente un concepto de documento que lo identifica con el escrito en soporte tradicional. La cuestión radica en saber si el escollo que supone la interpretación literal de la legalidad vigente es o no salvable. Para ello debemos tener en cuenta que la exacta significación de la ley no obedece solamente a un análisis exclusivamente gramatical y que es posible tomar en cuenta otros criterios como el teleológico y el sociológico. Con ayuda de ellos la interpretación puede ser diversa y en consecuencia el alcance que deba dársele al vocablo documento puede ser más amplio que el tradicional, sin que ello suponga una desvinculación de la ley (1999, 63 ss)

Contra la anterior posición sostiene Montero que según nuestro derecho positivo una forma de representación que no sea la escrita (...) no es un

documento. Esto es algo que hay que admitir guste o no guste, y que se impone al intérprete a no ser que éste no se sienta vinculado por la Ley (1988,145).

Respondiendo a este planteamiento, afirma la autora Sanchis, citando a Serra, "que una cosa son los conceptos dogmáticos y otra muy distinta la regulación positiva y si bien el Código Civil y el Código de Enjuiciamiento Civil, no podía lógicamente hacer referencia a los modernos medios reproductivos, y sus preceptos se refieren exclusivamente al único medio de reproducción usual en su época, la escritura (en soporte tradicional), ello no significa que cualquier avance técnico exija la regulación de un nuevo medio probatorio, sino más sencillamente que la doctrina y la jurisprudencia deben intentar adaptar dichos nuevos medios reproductivos a las leyes vigentes mientras éstas no sean objeto de la necesaria adaptación". (2000,76).

B. EL NUEVO DERECHO INFORMATICO.

El derecho informático es un tema bastante discutido en la doctrina, de allí que existen diversas definiciones.

El autor Peñaranda (2000,77) define el derecho informático como una ciencia que estudia la regulación normativa de la informática y su aplicación en todos los campos.

Por su parte, los autores Ocampo y Hernández, (1987,10) afirman que el derecho informático se refiere al tratamiento normativo que debe darse a los problemas jurídicos que suscita la informática.

Para los autores chilenos, Huerta y Líbano (1996, 56), el derecho informático es aquella rama del derecho que tiene por objeto la protección de los productos del ingenio humano, los cuales traducidos en información automática, se convierten en bienes jurídicos de incalculable valor.

Considera Carrasco (2000,77) que la anterior definición es demasiado restringida por cuanto no considera otros aspectos que integran el derecho

informático como es el valor probatorio del documento electrónico, comercio electrónico etc.

El mexicano Téllez (1994,58) define el derecho a la informática como el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática.

En opinión de Davara (1993,44) todos debemos trabajar para colaborar, para marcar bien claramente la diferencia entre los que es, lo que puede ser y lo que debe ser, orientando bien el camino que debe tomar la regulación jurídica del fenómeno informático en lo que hemos dado en llamar el derecho informático. Este autor no define el derecho informático, sino que solo señala que es necesario que se regule la informática.

Dentro de esta tendencia se encuentran Guibourg, Alende y Campanela quienes sostienen que la informática ha planteado al derecho problemas nuevos, que los juristas y legisladores se esfuerzan por resolver.
Estos autores coinciden en señalar que el derecho informático no es una rama autónoma, sin embargo aceptan cierta autonomía de este por conveniencias pragmáticas siempre que las circunstancias históricas así lo quisieren (1996,218).

En este sentido, sostiene Carrasco (2000,81) citando al autor peruano Salazar Cano, que es necesario enunciar las características del derecho informático, sin entrar a debatir el carácter autónomo del mismo. Estas características son las siguientes:

1. Se trata de un orden normativo particularmente nuevo comparado con otras disciplinas jurídicas.

2. Se trata de un derecho en permanente cambio, sin embargo todo derecho está en permanente cambio, por ello no será propio del derecho informático.

3. Se trata de un derecho que se ubica en un sin número de actividades tanto sociales como económicas, lo que lo convierte en un derecho de carácter general.

4. La unidad del derecho informático viene dada por la originalidad técnica impuesta por el fenómeno informático.

5. Se trata de un derecho complejo, toda vez que se interrelaciona con diversas ramas del derecho, como el derecho comercial, civil, procesal, internacional público, penal, etc.

En el VI Congreso Iberoamericano de derecho informático celebrado en Montevideo, Uruguay en 1998, el ponente Peñaranda Quintero sostuvo que la discusión de la autonomía del derecho informático se puede sistematizar en dos corrientes:

Una primera que sostiene la autonomía como una rama independiente y que constituye un cuerpo autónomo de normas jurídicas que tienen por objeto regular las actividades que derivan de la informática, dentro de un orden eficiente y justo.

Los argumentos que se esgrimen para sostener la autonomía se pueden ordenar de la siguiente manera:

a) El hecho de tener un carácter interdisciplinario no lo priva de la autonomía, ya que lo único importante es que esta rama debe sistematizar y reducir a una unidad, la pluralidad de elementos relacionados con el impacto social del fenómeno informático.

b) El derecho informático presenta bases conceptuales claras y con fundamento científico.

c) El aumento del desarrollo tecnológico constituye un elemento determinante para el surgimiento de esta rama, ya que surgen nuevas conductas que hacen necesaria su regulación.

d) Cumple con todos los supuestos que requiere una rama jurídica autónoma, o sea, una legislación especifica (campo normativo), un estudio particularizado de la materia (campo docente), investigaciones y doctrinas que tratan la materia (campo científico), instituciones propias que no se encuentran en otras áreas del derecho (campo institucional.

Por otro lado, se encuentran aquellos que le niegan autonomía al derecho informático y buscan la consagración desde el punto de vista de cada rama jurídica donde la actividad informática se encuentra presente, rechazando la integración de normas en un cuerpo aislado.

Los autores colombianos Ocampo y Hernández (1987, 11 y ss y los argentinos Guibourg, Alende y Campanella (1996,219 y ss) sostienen los argumentos para sostener la segunda postura basados en lo siguiente:

a) Un banco de datos puede estar relacionado con el derecho administrativo, penal, o privado, y de esta manera no se puede señalar que exista un área específica del derecho con mayor vocación que otra para regular el asunto concerniente al banco de datos.

b) La informática aporta a cada rama del derecho, cuestionando ciertas normas y proponiendo nuevas reglas.

c) Con el criterio que se utiliza para la individualización del derecho informático, se podrían imaginar diversas ramas de la ciencia del derecho. Así por ejemplo, el derecho automovilístico, sus temas se tomarían del derecho fiscal, comercial, penal, civil, administrativo etc.

d) Para que exista una rama jurídica autónoma es necesario que los principios que la informen hagan innecesaria su recurrencia a los principios de otra rama para la solución de los casos y ello no ocurre en el derecho informático.

No podemos negar que el derecho informático requiere un tratamiento sistemático de manera autónoma, pero no buscando una autonomía ontológica sino pragmática, a objeto de observar sus problemas desde una perspectiva globalizadora, sin embargo no podemos desconocer que el derecho informático contiene ciertos principios que le son propios como ocurre en materias como la contratación electrónica o el documento informático o electrónico y de concluir que tiene cierta autonomía potencial.

C. LA INFORMÁTICA Y EL DERECHO.

Dentro de los fenómenos más sorprendentes de la actual coyuntura de la bibliografía jurídica figura el de la escasez de fuentes sobre interacción entre la informática y el Derecho. El dato es relevante en un doble sentido, primero, por el contraste que ello supone respecto de la abundancia de publicaciones que, día a día, anegan nuestras bibliotecas jurídicas para tratar de argumentos consabidos, o de otros que, aún siendo novedosos, poseen una trascendencia notablemente inferior a la que reviste la tensión bipolar informática-Derecho en una sociedad post-industrial que se define a si misma como "informatizada".

Pero además, y éste sería el segundo motivo de relevancia aludida, este hecho es singularmente paradójico en la situación ambiental de la cultura jurídica del presente, cuya divisa cotidiana es la renovación de sus causas operativas a partir del acercamiento de las experiencias jurídicas más avanzadas.

Es notorio que los sistemas jurídicos más evolucionados, tienen como rasgo distintivo común su preocupación por la temática de las relaciones entre el mundo del derecho y el de los computadores electrónicos; preocupación materializada en un copioso elenco de libros y artículos, en la existencia de publicaciones periódicas orientadas al estudio del tema.

En este orden de ideas, sostiene el autor Bermejo que esta tecnología posmoderna, inicialmente reducida al papel de soporte o apoyo –y por tanto, con valor instrumental exclusivo– comienza a adquirir un relativo valor *in se* de insospechadas posibilidades, y las eventuales críticas que se puedan hacer, rayan en lo irracional y demagógico. Lo cierto es que, quiérase o no, el mundo de la información automatizada constituye uno de esos signos que caracterizan a la época postmoderna, y, para bien o para mal, es un mundo de profundo impacto en la vida de los hombres en las sociedades organizadas. La ciencia del derecho, cuya dimensión social y cultural es

indudable, no puede estar al margen de tales fenómenos de nuestro tiempo; el derecho debe estar allí, precisamente, para minimizar los riesgos porque sus ventajas no generan motivo alguno de importancia para nuestra ciencia. (1989, 113).

Sostiene el profesor Ortiz-Ortiz (2001, 20) que hasta ahora, las repetidas advertencias y las nuevas respuestas del Derecho ante el fenómeno de la informática se han quedado en el mero plano de la defensa del derecho a la privacidad o intimidad, sin embargo, la problemática tiene dimensiones mucho más profundas e implicaciones insospechadas, por lo que precisa los siguientes aspectos:

a) El nacimiento de una parte del derecho procesal que debe resolver los problemas relativos a los documentos informáticos como medio de prueba del nacimiento o extinción de las obligaciones; además, los problemas relativos a la llamada "firma electrónica", y sus efectos jurídicos, entre otros aspectos que, por abusar del término, hemos llamado "derecho procesal informático";

b) En segundo lugar, el derecho de autor tiene, en las creaciones artísticas, literarias y científicas publicadas en Internet, una doble tarea:

precisar su propio ámbito de aplicación, y sus regulaciones específicas. Muy cerca, sin llegar a identificarse, surge la problemática de las marcas y las patentes que hacen posible el comercio electrónico cada vez de mayor presencia en nuestros pueblos iberoamericanos;

c) El derecho penal cuenta con al extraordinario reto de adelantarse a las "creaciones" delictivas, esto es, debe prever los "tipos" y las agravantes o atenuantes que pudieran surgir en la penalización; se trata de una nueva "rama" del derecho penal para combatir los llamados "delitos informáticos" o "criminalidad informática", tomando en cuenta que para tales nociones se ha querido sustantivizar el medio empleado para la comisión del delito; y por último,

d) La tutela de los derechos fundamentales de la persona (tanto las jurídicas como las personas naturales frente a la injerencia en su esfera de derechos, no sólo en lo que respecta de la intimidad sino también otros derechos como la propiedad, el honor, la reputación, etc.)

Sostiene el autor Carrasco que a través del tiempo hemos visto que un lápiz constituye una extensión de nuestras manos, la radio de nuestra voz, una bicicleta de nuestras piernas y la computadora es una extensión de nuestro

cerebro. Ella constituye en palabras de Guibourg, Alende y Campanella (1996,70) una maquina de pensar, puesto que reproduce y multiplica alguna de las funciones de la mente y hasta se proyecta no sin algún optimismo hacia la idea de inteligencia artificial. Efectivamente con el ordenador lo que pretende es tratar de emular el pensamiento humano en determinados aspectos, facilitando el desarrollo de las actividades humanas. (2000,16).

Siguiendo el autor Rivera (1995,3) entre informática y derecho existen dos tipos de interrelaciones. En primer lugar, tenemos un aspecto instrumental de la informática al servicio del derecho, que implica una incursión de la informática jurídica y en segundo lugar, si se considera a la informática en todos sus aspectos como objeto del derecho, estaremos frente al campo del derecho informático. Podemos decir, que así como en la informática jurídica, es la informática la que esta al servicio del derecho, en el caso del derecho informático los papeles se invierten. Hoy se habla con reiterada insistencia, del surgimiento y reconocimiento de un nuevo derecho, "el derecho informático", que posee todas las características de un derecho especializado.

En definitiva, el problema de la protección del hombre, ante ciertas tecnologías que conciernen más particularmente al individuo, porque ellas

influyen sobre su persona, física o moral, sigue siendo una preocupación dentro del derecho moderno, que pretende aglutinarse en torno al mencionado derecho informático.

D. EL DERECHO INFORMÁTICO Y LA INFORMÁTICA JURÍDICA

Sobre este punto sostiene el autor Gustavino, (1987,26 SS) que en esta aproximación a la informática jurídica existen algunos problemas esenciales relacionados con la tutela legal de los instrumentos informáticos, la informática y la protección de la intimidad y de los datos reservados, los contratos informáticos, los delitos informáticos, la responsabilidad civil de los daños referidos a la informática y el derecho procesal informático.

Es útil la distinción entre informática jurídica y derecho informático. La primera concierne a la informática como avanzado medio técnico que proporciona auxilio y servicio a las diversas actividades relacionadas con el derecho. El segundo, el derecho informático, es el conjunto de normas y principios jurídicos que tienen como objeto de regulación a la informática.

El profesor Ortiz-Ortiz (2001, 22) señala que puede hablarse del derecho informático y de la informática jurídica, según el cual el derecho informático se refiere a las diversas áreas del derecho que se ven afectadas por la información automatizada, esto es, aspectos procesales, penales, mercantiles, tributarios y fiscales, entre otros; y la informática jurídica se refiere a los diversos usos de los recursos tecnológicos que debe ser regulados por el derecho, tales como el servicio informático, las regulaciones sobre la transmisión de datos, la automatización del poder judicial, entre otros.

La informática jurídica contiene dos grandes aproximaciones como señala Carrasco (2000,48):

a) Aquella que busca aplicar al derecho la lógica y otras técnicas de formalización, con vista al empleo de los medios electrónicos.
b) La otra aproximación busca aplicar la acción de los computadores al campo del derecho, incluida aquella acción tendiente a la construcción y utilización de *software* destinado a lograr ese objetivo.

En conclusión, podemos decir que la informática resulta de la aplicación de los avances tecnológicos al tratamiento de la información.

E. ASPECTOS DEL DERECHO INFORMÁTICO

Hoy, el derecho informático ha tenido una mayor difusión a nivel mundial. El catedrático Ortiz-Ortiz, (2001, 25) en su obra Habeas Data, Derecho Fundamental y Garantía de Protección de la Personalidad (Derecho a la Información y Libertad de Expresión) realiza un análisis de los aspectos que debe afrontar la ciencia del derecho en general y en particular el derecho procesal, de autor, penal mercantil y constitucional.

1. Los delitos penales y la criminalidad informática

Sostiene el profesor Ortiz-Ortiz (2001,26) que una de las áreas más importantes donde se ha visto el impacto del desarrollo informático es en el derecho penal debido a que se hace necesario la regulación precisa de los tipos penales para salvaguardar bienes jurídicos que importan a la sociedad

En este sentido afirma el autor Rivera (1995,11) que el uso de las computadoras ha dado lugar a este fenómeno de dimensiones nuevas y desconocidas llamado delito informático, consecuencia del desarrollo de la

tecnología que ha dado lugar al nacimiento de delincuencias antes impensable, la manipulación fraudulenta de las computadoras con animo de lucro: la destrucción de programas de datos y el acceso y la utilización indebida de información, que puede afectar a la esfera de la privacidad, o causar importantes daños materiales y morales. Pero no solo la cuantía de los daños es infinitamente mayor a la que se ocasiona por la delincuencia tradicional, sino que son mucho más elevadas las posibilidades de que lleguen a descubrirse. al ser la información un bien inmaterial, esto acarrea consecuencias, que al actuar delictivo contra él, se elabore también inmaterialmente. Por ejemplo, el crear un programa para delinquir mediante el uso de una computadora o sus derivados, hace que el objeto con el cual realizamos el ilícito sea también inmaterial, rasgo demostrativo de lo lejos que nos podemos encontrar de la tipicidad penal en el área de la informática, sin embargo encontramos casos que son realmente claros como la fabricación de una bomba de tiempo, que es un programa de computación por el cual todo un sistema puede desaparecer (nos referimos al soporte lógico del sistema, al *software*) e incluso dañar el soporte físico (*hardware*).

En la actualidad, existe la legislación penal sobre protección a la criminalidad informática en distintos países europeos como España, Alemania, Austria, Francia, que han creado tipos penales específicos en la materia señalada,

igualmente ocurre en países como Chile, Argentina Uruguay y en Venezuela recientemente se dictó la Ley especial sobre los delitos informáticos, y estamos a la espera de la modificación del Código Penal vigente.

2.- Delincuencia y criminalidad informática

Existen una serie de temas nuevos en el derecho penal que son consecuencia de cambios político-institucionales, así surgen casos de necesidades de combatir organizaciones criminales de larga data, que requieren repensar el derecho penal tradicional. Por ejemplo el crimen organizado y la mafia requieren nuevas tipificaciones penales para combatirlas con eficacia. En nuestro país existen muchas conductas delictuales que no han sido tipificadas como tales, esto hace que el delito informático, su existencia, su prevención y hasta su persecución dependan de muchos factores, entre otros de la recepción de los cambios tecnológicos en el derecho sustancial pero también en el derecho formal y en las organizaciones judiciales y fuerzas de prevención.

El autor Quiñonez (1987,4 ss) vincula la delincuencia o criminalidad informática con la "delincuencia de cuello blanco "por la manera ingeniosa y complicada que se emplea en la comisión de actos irregulares, aunada al

carácter complejo y a la diversidad de medios de que disponen (...) dentro de la delincuencia económica se ubica la delincuencia informática, esto es, la que emplea nuevas técnicas de las computadoras para fines ilícitos".

Señala el autor Barriuso (1996,246) que la informática y los dispositivos electrónicos suponen, por sus características, un poder de amplificación de las consecuencias de los fraudes y delitos informáticos como objetos y como instrumentos de los mismos, lo que justifica a la vista de ello, una regulación y tipificación especifica con una definición clara del bien jurídico a proteger, pero que deje la posibilidad de tipificar otros tipos delictivos que surjan.

3 El Delito Informático

Existe una serie de características de la criminalidad informática que debemos precisar para llegar al concepto de delito informático.

Comenzaremos precisando que cuando surgen estos delitos denominados delitos informáticos se requiere de la reforma de la legislación penal vigente y a veces la civil para introducir nuevos conceptos que cumplan con las exigencias que brinden la seguridad y finalidad de la Ley.

A manera de ejemplo cita el autor argentino Palazzi el caso del hurto de energía eléctrica y más modernamente el caso de pulsos telefónicos o de señales de televisión. El problema fundamental que planteaba la electricidad al jurista era su incorporeidad característica que es aplicable actualmente a la información almacenada en un ordenador, sin embargo la solución fue interpretar el valor que representaba la cosa, es decir, la energía eléctrica Aplicando este concepto se ha determinado que eran susceptibles de ser hurtadas las señales de teléfono, las señales de video cable y la electricidad. (2000,49).

Por otra parte en los últimos años se ha notado un aumento de la criminalidad informática, ello se debe al gran desarrollo de la informática y la telemática, haciendo cada vez más común el uso de ordenadores en las labores cotidianas.

Ahora bien, existe otro tipo de problemas, como son los problemas probatorios que suscitan esta clase de delitos los que impiden determinar quien fue el responsable o que el hecho ocurrió por un accionar doloso y no por una falla del sistema.

Para continuar el tema, es preciso señalar, que el delincuente informático posee ciertas características, de allí que el sujeto pasivo este conformado por un determinado grupo de personas con una inteligencia y educación que superen el común y con vastos conocimientos informáticos.

En cuanto al sujeto pasivo se ha determinado que las entidades financieras, y el Estado son las victimas de la criminalidad informática, ello ha llevado a constituir agravantes cuando el bien jurídico sea propiedad del estado y actualmente cualquiera que opere con ordenadores puede ser victima del delito informático.

Además de los problemas mencionados anteriormente, existen otros como la extraterritorialidad, la dificultad para la investigación del delito informático y los problemas que plantea internet y las autopistas de la información al derecho penal.

En Venezuela fue dictada la Ley Especial Contra los Delitos Informáticos el día 30 de octubre de 2001 cuyo objeto es la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus

componentes, o de los delitos cometidos mediante el uso de dichas tecnologías.

Establece dicha ley en su articulo 4 que las sanciones por los delitos serán principales y accesorias.

> "Las sanciones principales concurrirán con las penas accesorias y ambas podrán también concurrir entre si, de acuerdo con las circunstancias particulares del delito del cual se trata, en los términos indicados en la presente ley."

En cuanto a la responsabilidad de las personas jurídicas, menciona en su artículo 5:

> "Cuando los delitos previstos en esta ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, estos responderán de acuerdo con su participación culpable.
>
> La persona jurídica será sancionada en los términos previstos en esta ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en un interés exclusivo o preferente."

4. Clasificación de los delitos informáticos.

Los autores extranjeros han diferenciado las distintas clases de delitos informáticos, así vemos como Téllez, citado por Ortiz-Ortiz (2001,39) clasifica los delitos informáticos en atención a dos criterios: como instrumento o medio, o como fin u objetivo:

a) Como instrumento o medio: en esta categoría tenemos a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, así:

1) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).

2) Variación de los activos y pasivos en la situación contable de las empresas.

3) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etc.)

4) "Robo" de tiempo de computadora.

5) Lectura, sustracción o copiado de información confidencial.

6) Modificación de datos tanto en la entrada como en la salida.

7) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto se le conoce en el medio como el método del "Caballo de Troya").

8) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la "técnica de salami".

9) Uso no autorizado de programas de cómputo.

10) Introducción de instrucciones que "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios, tales como consulta a su distribuidor.

11) Alteración en el funcionamiento de los sistemas, a través de los cada vez más temibles virus informáticos.

b) . Como fin u objetivo perseguido por el autor del delito: en esta categoría se enmarcan las conductas criminales que van dirigidas en contra de la

computadora, accesorios o programas como entidad física. Algunos ejemplos, son los siguientes:

1) Programación de instrucciones que producen un bloqueo total al sistema.

2) Destrucción de programas por cualquier método;

3) Daño a la memoria;

4) Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etc.).

5) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados; y

6) Hurto de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

Para el autor Sloan citado por Palazzi (2000,39) hablar de delito informático no implica solo un delito cometido por medio de computadoras.

Un delito informático (*computer crime*) consiste en el uso de una computadora como instrumento de un delito económico. Cita un ejemplo que es el de realizar cambios no autorizados al programa de computación para transferir fondos de una cuenta inactiva a una cuenta propia. Explica que las

computadoras pueden tener varios roles en el delito, estos son como: a) objeto; b) sujeto; c) instrumento; y como d) símbolo.

El autor Ulrich Sieber publico dos obras, una en 1977 y otra en 1986, sobre trabajos de investigación y artículos convirtiéndose en uno de los grandes especialistas en delito informático. En su último trabajo preparado para la Comisión Europea por la universidad de Wurzburg, en enero de 1998, arriba al siguiente esquema, compartido por Palazzi (2000,43)

a) Protección de la privacidad.

b) Delitos económicos.

c) Protección de la propiedad intelectual.

d) Contenido ilegal y nocivo de las autopistas de la información.

e) Derecho procesal penal.

f) Derecho y seguridad.

5) Nuestra clasificación.

La Ley Especial Contra los Delitos Informáticos clasifica los delitos informáticos de la siguiente manera:

1. -Delitos contra los sistemas que utilizan tecnologías de la información.

a) Acceso indebido.

b) Sabotaje o daños a sistemas.

c) Favorecimiento culposo del sabotaje o daños.

d) Acceso indebido o sabotaje a sistemas protegidos.

e) Posesión de equipos o prestación de servicios de sabotaje.

f) Espionaje informático.

g) Falsificación de documentos.

2.- Delitos contra la propiedad.

a) Hurto.

b) Fraude.

c) Obtención indebida de bienes o servicios.

d) Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.

e) Apropiación de tarjetas inteligentes o instrumentos análogos.

f) Provisión indebida de bienes o servicios.

g) Posesión de equipos para falsificaciones.

3.- Delitos contra la privacidad de las personas y de las comunicaciones

a).Violación de la privacidad de la data o información de carácter personal.

b) Violación de la privacidad de las comunicaciones.

c) Revelación indebida de la data o información de carácter personal.

4.- De los delitos contra niños, niñas o adolescentes.

a) Difusión o exhibición de material pornográfico.

b) Exhibición pornográfica de niños y adolescentes

5.- De los delitos contra el orden económico.

a) Apropiación de propiedad intelectual.

b) Oferta engañosa.

En nuestra opinión la vigencia de la Ley Contra Delitos Informáticos debe completarse con la reforma del Código Penal y tal vez el Civil para que pueda gozar de plena aplicación.

6). Nuestro código penal

Uno de los países con mayor atraso en esta materia es Venezuela.
El Código penal contiene algunas disposiciones relativas a la vida privada, tipificando los delitos contra la inviolabilidad del domicilio (artículos 184 y 185) y el secreto documentario y de correspondencia (artículos 186 al 191).

El profesor Ortiz-Ortiz (2001, 49 ss) señala que con respecto a las comunicaciones, el Código Penal recoge alguna normativa en este sentido al tipificar:

> "El que haya dañado los puertos, muelles, aeropuertos, oleoductos, gasoductos, las oficinas, talleres, obras, aparatos, tuberías, postes, cables y otros medios empleados por los sistemas de transporte o comunicación será penado con prisión de dos a cinco años",

y que a decir de Quiñónez, la norma es insuficiente para hacer que su penología corresponda a la dimensión de los valores por ella protegidos.

En 1991 se dictó la Ley Sobre Protección a la Privacidad de las Comunicaciones; la iniciativa de la Ley estuvo a cargo de la Comisión de Política Interior e ingresó a la Cámara de Diputados el 14 de mayo de 1991; las discusiones reglamentarias se le dieron el 14 y el 13 de Junio del mismo año, pasando a la Cámara Revisora el 18 de del mismo mes. En la Cámara del Senado se le dan las dos discusiones debidas el 27 de Junio de 1991 y el 31 de Octubre del mismo año, para que por fin en Sesión Conjunta del Congreso se sancionara el 21 de Noviembre de 1991 promulgada por el Ejecutivo el 16 de Diciembre y publicada en Gaceta Oficial Nº. 34.863 de esa misma fecha.

El 12 de junio de 2000, se dictó la Ley de Telecomunicaciones (GO r54r45 nº 36.970 de la misma fecha), cuyo objeto era "establecer el marco legal de regulación general de las telecomunicaciones, a fin de garantizar el derecho humano de las personas a la comunicación y a la realización de las actividades económicas de telecomunicaciones necesarias para lograrlo, sin más limitaciones que las derivadas de la Constitución y las leyes" (artículo 1º) excluyéndose de ese objetivo la regulación del contenido de las

transmisiones y comunicaciones cursadas a través de los distintos medios de telecomunicaciones, la cual habrá de regirse por las disposiciones constitucionales, legales y reglamentarias correspondientes.

La mencionada ley tiene como objetivos generales los siguientes:

1. Defender los intereses de los usuarios, asegurando su derecho al acceso a los servicios de telecomunicaciones, en adecuadas condiciones de calidad, y salvaguardar, en la prestación de estos, la vigencia de los derechos constitucionales, en particular el del respeto a los derechos al honor, a la intimidad, al secreto en las comunicaciones y el de la protección a la juventud y la infancia. A estos efectos, podrán imponerse obligaciones a los operadores de los servicios para la garantía de estos derechos.

2. Promover y coadyuvar el ejercicio del derecho de las personas a establecer medios de radiodifusión sonora y televisión abierta comunitarias de servicio público sin fines de lucro, para el ejercicio del derecho a la comunicación libre y plural.

3. Procurar condiciones de competencia entre los operadores de servicios.

4 Promover el desarrollo y la utilización de nuevos servicios, redes y tecnologías cuando estén disponibles y el acceso a éstos, en condiciones de igualdad de personas e impulsar la integración del espacio geográfico y la cohesión económica y social.

5. Impulsar la integración eficiente de servicios de telecomunicaciones.

6. Promover la investigación, el desarrollo y la transferencia tecnológica en materia de telecomunicaciones, la capacitación y el empleo en el sector.

7. Hacer posible el uso efectivo, eficiente y pacífico de los recursos limitados de telecomunicaciones tales como la numeración y el espectro radioeléctrico, así como la adecuada protección de este último.

8 Incorporar y garantizar el cumplimiento de las obligaciones de Servicio Universal, calidad y metas de cobertura mínima uniforme, y aquellas obligaciones relativas a seguridad y defensa, en materia de telecomunicaciones.

9. Favorecer el desarrollo armónico de los sistemas de telecomunicaciones en el espacio geográfico, de conformidad con la ley.

10. Favorecer el desarrollo de los mecanismos de integración regional en los cuales sea parte la República y fomentar la participación del país en organismos internacionales de telecomunicaciones.

11. Promover la inversión nacional e internacional para la modernización y el desarrollo del sector de las telecomunicaciones.

II. NATURALEZA JURÍDICA DEL DOCUMENTO ELECTRÓNICO Y VALOR PROBATORIO.

Para Carnelutti, (1982, 121) la prueba documental se ha caracterizado siempre por la seguridad que proporciona a quien la tiene a su favor. Esa seguridad radica en una característica especifica de este tipo de prueba: el ser preconstituida, es decir, el fijarse con anterioridad al momento en que surge el conflicto. Ello indudablemente garantiza su sustracción a todas las influencias corruptoras, que los intereses en conflicto dentro del proceso pueden ejercitar. A su vez esa seguridad tiene dos componentes: fidelidad y perdurabilidad.

La fidelidad consiste en la seguridad de que lo representado coincide con lo que efectivamente se realizó y que, al quedar plasmado, no puede quedar comprometido por la acción del tiempo sobre la memoria humana.

La perdurabilidad la proporciona la constante disponibilidad de lo representado tal y como acaeció en cualquier momento puede acreditarse la existencia del derecho o que las cosas sucedieron de una determinada manera favorable a nuestros intereses.

Como sostiene Sanchis, (1999,64) es precisamente esa seguridad la que se pone en tela de juicio con relación a los modernos documentos. Se dice que al ser fácilmente manipulables y no estar garantizada su perdurabilidad a través del tiempo, su seguridad no queda en absoluto garantizada y por tanto no es asimilable a la de un documento escrito tradicional.

Examinemos ambos componentes por separado.

En lo relativo a la fidelidad de las modernas reproducciones documentales hay que decir que la creencia de que un documento en soporte informático es fácilmente manipulable, no es más que eso, una creencia, con poca o nula justificación práctica.

Para adulterar un documento informático se necesitan ciertos conocimientos técnicos, y la manipulación de un soporte informático, puede llegar a ser imposible si el documento está protegido por un código de ingreso (clave secreta o *password*) que no logra descubrirse, o mediante encriptación (técnica mucho más segura que hace que el documento resulte indescifrable para quien no conozca la secuencia del algoritmos elegida). También es posible utilizar métodos basados en la biometría que hacen que pueda determinarse con toda precisión la identidad de la persona que accede a un sistema electrónico para emitir un mensaje y al mismo tiempo la autenticidad

del mensaje transmitido y recibido; en cambio para falsear un documento escrito en soporte tradicional, a pesar de ser necesarias ciertas cualidades, el material usado es mucho más accesible (máquina de escribir, impresora, papel, liquido etc.)

En los documentos digitales existe un peligro grave con la perdurabilidad y para salvaguardarla se deben tomar ciertas precauciones que no siempre se observan.

El principal problema que tiene la perdurabilidad de estos documentos es doble: de un lado está su fragilidad física, la cual puede paliarse, realizando cada cierto tiempo copias, el segundo es más complicado de evitar. Como dice, un especialista en la materia, Rothemberg, (1995,8) en su obra ¿Son perdurables los documentos digitales?:"Los documentos digitales se quedan anticuados rápidamente y no logran mantenerse legibles durante la centésima parte del tiempo que lo ha sido la piedra Roseta, es decir, más de veintidós siglos. Con un ejemplo ilustra las informaciones anteriores: Año 2045. Mis nietos (que no han nacido aún) están explorando el desván de mi casa (que no he comprado todavía).

Descubren una carta fechada en 1995 y un disco *CD-ROM.* La carta dice que el disco contiene un documento en el que se da una clave para heredar, mi fortuna (que no he ganado aún). Mis nietos sienten viva curiosidad, pero jamás, salvo en viejas películas han visto un disco compacto, salvo en viejas películas. Aún cuando localizaran un lector de discos adecuado ¿Cómo lograrían hacer funcionar los programas necesarios para la interpretación del contenido? ¿Cómo podrán leer mi anticuado documento digital? De no ser por la carta explicativa, mis nietos no tendrían motivo para pensar que mereciera la pena descifrar el disco. La carta posee la envidiable propiedad de ser legible sin máquinas, instrumentos o conocimientos especiales, aparte del propio idioma."

Sigue diciendo este autor que debido a que la información digital puede copiarse y recopilarse a la perfección se álava a menudo su incuestionable longevidad. Pero la verdad es otra. Dado el carácter mudable de programas y circuitería, dentro de cincuenta años lo único directamente inteligible será la carta. El contenido de casi todos los soportes digitales se esfuma mucho antes que las palabras escritas en papel de calidad.

Para que pueda ser legible el documento de que hablamos se deberá incluir en el mismo toda la base informática requerida para extraer el contenido del

programa sin alterar su forma (ya que alteraciones en la forma que pueden modificar el contenido) junto con la información necesaria para generar un emulador capaz de ejecutar los programas originales o conseguir un ordenador antiguo en buen uso. Tales precauciones habitualmente no se toman con los riesgos que ello conlleva.

Resulta que la fidelidad de los documentos no tiene porque ser necesariamente menor que la de los tradicionales. Mientras que la perdurabilidad, es sensiblemente inferior. La conclusión es, pues, que los nuevos documentos no gozan de los mismos niveles de seguridad que los tradicionales; sin embargo, con las precauciones adecuadas, la seguridad tiene un nivel aceptable. Además debe tenerse en cuenta que la seguridad de los soportes informáticos constituye en la actualidad un campo fértil de investigación que previsiblemente, dará frutos en un futuro próximo.

A. AUTENCIDAD DEL DOCUMENTO ELECTRÓNICO.

Siguiendo la opinión del autor Barriuso, (1986, 235) es criterio jurisprudencial sentado que para la eficacia de los derechos u obligaciones constituidos en documento privado es esencial la firma del obligado. Este criterio tomado literalmente, por si mismo, invalidará los efectos de un documento sin firma,

pero si nos atenemos a la semántica de la palabra firma y su contexto, vemos que la característica principal de la firma es dotar de autenticidad lo suscrito con ella. Sentado esto, vemos que por medio de dispositivos electrónicos de encriptación podemos dotar de señas de autenticidad a un documento.

Algunos autores dudan en la autoría de la contraseña electrónica de validación del documento, pues en el caso de la firma autógrafa el problema no existe, porque solo la mano de la persona del autor puede firmar dicen, y para su comprobación existiría, caso de negarse, la prueba pericial de caligrafía; pero en el caso del dispositivo electrónico se puede decir que cualquier persona puede accionar el mecanismo de validación, y que lo único que demostraría es que ha sido realizado por tal o cual persona, lo que podría crear incertidumbre; con lo que no estamos de acuerdo, pues si bien en un caso el procedimiento es electrónico y en otro es manuscrito, los dos son manufacturados y no por eso pierde autenticidad, autoría y por ende obligatoriedad, ya que el acceso o la posibilidad de imprimir o plasmar esa contraseña electrónica está vedada a quien no disponga del método, clave, huella dactilar, genoma etc., para su obtención, y entonces todo radicaría en la prueba pericial, que tendría que ser informático-electrónica en lugar de caligrafía, en el caso de negar la autoría el titular de una clave o

procedimiento de validación electrónico. Por ello, se debe invocar y aportar en juicio estos nuevos elementos probatorios con base a los fundamentos jurídicos expuestos de pertinencia, indefensión y adecuación real y social, disponiendo de identificación y autoría y no violando ningún precepto en su obtención.

Considera el autor Marchena, que las nuevas tecnologías de la información, unidas a otras técnicas, ya antiguas, como la criptografía, proporcionan fiabilidad al documento, muy superior en ocasiones, mediante procedimientos lógicos de control a la que proporciona la firma y ofrecen caracteres de autenticación, con garantías que superan a los errores humanos, fácilmente cometibles. La fórmula de la firma electrónica, registrada por diferentes métodos y técnicas en un fichero público de control, modificada hasta tecnológicamente por razones de seguridad, nos llevaría a la autenticación de los documentos electrónicos mediante medios informáticos. (2000, 156).

No se plantea ningún problema en el intercambio de documentos en redes cerradas, esto es, en el intercambio de documentos, incluso en el pago electrónico, entre intervinientes que han aceptado previamente este sistema de comunicación, de compromiso y de pago; en ellas, en las redes cerradas,

se establecen sistemas o elementos de control y verificación, previamente diseñados y aceptados por ambas partes, que basados en la mutua confianza raramente ofrecen problemas; es, por tanto, una cuestión de confianza más que de seguridad.

Los problemas y las discrepancias, pueden surgir cuando utilizamos los mismos elementos en redes abiertas en los que los intervinientes aceptan unas reglas de juego pero en las que falta la premisa de la confianza ya que en muchas ocasiones, teóricamente en todas ni siquiera se conocen.

Es por ello que, en el primero de los casos, la utilización de técnicas criptográficas, que mediante el cifrado ofrecen una protección de seguridad lógica a la información, actúa como medida de seguridad en el teórico viaje que los datos efectúan a través de la red; de esta forma, las técnicas criptográficas, en su aceptación genérica utilizan solamente como medida de seguridad pero no como creadoras de confianza.

Ahora bien, dentro de las técnicas criptográficas como una aplicación más, o como una aplicación distinta, también aparece la llamada firma digital como generadora de confianza; distinguiremos así la seguridad de la confianza y la protección criptográfica de la firma digital.

Mediante el cifrado del texto, utilizando la criptografía, se protege a la información del acceso, malintencionado o no, de quien no está autorizado para ello, y mediante la firma digital añadiremos al texto una información que se identifica con la persona que emite el mensaje, que se ratifica en el contenido, y las que se asocian a los posibles compromisos y responsabilidades que contenga. Vemos de esta forma que la firma digital cumple la misma función que la firma manuscrita y solamente nace la necesidad de explicarla porque la firma, como tal, se encuentra asociada popularmente a la escritura de papel y de puño y letra.

Conviene apuntar que mediante controles tecnológicos y técnicas criptográficas, se puede "garantizar" la autenticidad de un documento electrónico con un alto grado de seguridad en lo que podíamos llamar "el notario electrónico"; la firma electrónica, con las garantías exigidas por una cada vez más necesaria seguridad jurídica, puede abrir un difícil y tortuoso camino que deje en "entredicho" de seguridad de la fe pública tradicional; la seguridad física y lógica, y consecuentemente jurídica, que puede proporcionar la electrónica, es sorprendente y abre nuevos campos de estructuración, interpretación e incluso, creación del derecho.

El problema no está en la electrónica, ni en las comunicaciones, y, es posible que ni siquiera en la legislación, el problema es de formación y adecuación de personas y medios a la exigente realidad que puede proporcionar hasta una mayor credibilidad al derecho y a la administración de justicia, las nuevas tecnologías de la información y las comunicaciones, unidas a otras técnicas, dan fiabilidad al documento -muy superior- en ocasiones a la de la firma mediante procedimientos lógicos de control basados, como método idóneo de seguridad, en la criptografía, altamente fiable para proteger la información y que, adecuadamente normado y aceptado, proporciona seguridad sobre el contenido del mensaje y es camino lógico hacia la autenticación electrónica.

D. LA FIRMA ELECTRÓNICA EN VENEZUELA

En Venezuela se dictó el Decreto con rango y fuerza de ley, denominada Ley sobre Mensaje de Datos y Firmas Electrónicas cuyo objeto es otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y los certificados electrónicos.

El Decreto-Ley es aplicable a los mensajes de datos y firmas electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los mensajes de datos y firmas electrónicas.

La ley reconoce, sin embargo, que la certificación a que se refiere la ley, no excluye el cumplimiento de las formalidades de registro público o autenticación que de conformidad con la ley, requieran determinados actos o negocios jurídicos.

La firma electrónica es diferente cada vez que la hace una persona, es decir, esta vinculada al documento y por lo tanto son movimientos de la mano que se graban electrónicamente cada vez que se hacen, de modo que si la firma esta ligada a un documento, la persona entonces esta firmando distinto cada vez que hace un documento, esto esta garantizado con un certificado digital.

El certificado digital de asignación de firma, garantiza que cuando una persona envía un mensaje a un destinatario utiliza una clave atribuida, que dice que el destinatario es tal, de modo que el único que va a recibir y

descifrar el mensaje es el destinatario porque tiene la clave privada, es como la llave que le va a permitir descifrar el mensaje.

La Ley sobre Mensaje de Datos y Firma Electrónica extiende sus efectos a "todo sujeto jurídicamente hábil, bien sea natural, jurídica, pública, privada, nacional o extranjera, susceptible de adquirir derechos y contraer obligaciones", y define como "Mensajes de Datos" a toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

La firma electrónica es la información creada o utilizada por el signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

Es de observar que la firma sólo autentica "autoría" del documento y deja a salvo la veracidad del contenido. En efecto, el artículo 4º establece la eficacia probatoria de la firma electrónica en el siguiente sentido:

En cuanto a la eficacia probatoria, el artículo 4, establece:

> "Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.
> La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas."

Ahora bien, cuando, para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en esta ley; y cuando, para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un Mensaje de Datos al tener asociado una Firma Electrónica.

El Presidente de la República, dictó el Decreto con Fuerza de Ley nº 37.148 del veintiocho (28) de febrero de 2001 sobre Mensajes de Datos y Firmas Electrónicas, cuyo ámbito de aplicación es:

> "El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos y Firmas Electrónicas."

En nuestra ley se define a la firma electrónica como la Información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

C -BENEFICIOS DE LA FIRMA ELECTRÓNICA.

Al facilitar la autenticación a distancia entre partes que no necesariamente se conocen previamente, las firmas digitales constituyen el mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas. Por ello constituyen un elemento clave para el desarrollo del comercio electrónico en Internet.

En el ámbito nacional el comercio electrónico ya se está manifestando, existiendo supermercados, aerolíneas, agentes bursátiles y bancos que ofrecen sus productos y servicios directamente por Internet permitiendo así la compra de alimentos y artículos del hogar, de pasajes aéreos, de títulos

valores bursátiles y de transferencias de fondos entre cuentas bancarias y el pago de facturas de servicios.

A título de ejemplo puede mencionarse el efecto del comercio electrónico en Internet respecto del ámbito bursátil, para el cual el valor monetario de las transacciones de compra-venta de títulos valores iniciadas desde Internet en los EE.UU. en 1997 ascendió a 120 mil millones de dólares, estimándose que tal cifra se triplicará para 1998 (según el periódico "La Nación", página 23, Sección 5, Suplemento Informático del 13 de abril de 1998).

El comercio electrónico no es el único beneficiario de la firma digital. Actualmente las empresas y los organismos públicos de nuestro país se encuentran con grandes archivos contentivos de documentos en soporte de papel, que ocupan gran espacio en las oficinas impidiendo el desarrollo y modernización de las mismas. Los requerimientos legales que exigen la utilización del papel con firma manuscrita, impiden la implementación de modernos sistemas informáticos mediante los cuales se podría acceder a documentos a distancia y a la información en forma inmediata, dando lugar por ejemplo a nuevas modalidades de desempeño laboral como ser el tele-trabajo (*"tele-commuting"*).

Y es aquí donde se produce el mayor beneficio de la utilización de la firma digital, tanto estas nuevas modalidades de trabajo como el incremento en la velocidad de circulación de la información que permite hacer factible el documento digital permitirían que las organizaciones de nuestro país ofrezcan un mejor nivel de servicios a sus clientes y simultáneamente reduzcan sus costos, aumentando su productividad y su competitividad en lo que hoy son mercados cada vez mas globalizados y competitivos.

D. LAS FIRMAS ELECTRÓNICAS Y LAS AUTORIDADES CERTIFICADORAS.

En cuanto a las entidades certificadoras y la fe pública el autor chileno Jijena considera, que al lograrse con la emisión de un certificado que el receptor de un mensaje sepa individualmente que el emisor del mismo es realmente quien dice ser y que éste, a su vez, posteriormente no puede negar o repudiar el envío, se alcanzan mayores grados de confianza en las relaciones comerciales electrónicas o virtuales. En definitiva, el objetivo buscado es conferir fiabilidad a las relaciones comerciales establecidas mediante firmas electrónicas entre los usuarios de *internet* o de redes privadas. (2002,141,142).

Como la transposición mecánica de una firma manual realizada sobre papel y replicada por el ordenador a un documento informático no es suficiente para garantizar los resultados tradicionalmente asegurados por la firma ológrafa, se crea la necesidad de que existan entidades que certifiquen la validez de esas firmas. La trascendencia pública de la función de los prestadores de servicios de certificación, en consecuencia, pasa por el hecho de que cuando certifican dígitos o algoritmos y la pertenencia de esos dígitos a personas (naturales o jurídicas) concretas y determinadas por sus características propias, titulares de las llaves públicas, están ejerciendo la potestad jurídica de otorgar fe pública en el marco de las transacciones comerciales.

La firma del documento ha tenido siempre una doble finalidad, por un lado identifica a las partes y por el otro se aprueba su contenido.

Ahora bien, los documentos electrónicos carecen de firma autógrafa y por ello se ha llegado hablar de crisis de suscripción. Sin embargo, la doctrina y la jurisprudencia han asimilado los documentos electrónicos con los documentos tradicionales.

La ausencia de suscripción en los mensajes electrónicos, se subsana con la demostración de la exclusividad en el uso del instrumento técnico, que permite identificar el origen o procedencia del documento. Otra forma de demostrar la autoría de un documento electrónico, es la firma digital, pues ella permite firmar un documento en el espacio.

Considera Martínez (2002,142) que una firma electrónica sería cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones de la firma manuscrita.

Una clase particular de firma electrónica es la firma digital. Estas firmas digitales son, tecnológicamente, especificas pues se crean utilizando sistemas de criptografía asimétrica o de clave pública. Este sistema de claves públicas (basado en el uso de claves asociadas: una clave privada que se mantiene y una clave pública, libremente accesible), permite realizar firmas digitales que pueden ser, en el comercio y en el derecho , tanto o más útiles , eficaces y seguras que la firma de papel o manuscrita. (1988, 37,39).

Un ejemplo mencionado por Briceño, con ocasión de un foro celebrado en el IESA el 4 de agosto de 1999, titulado comercio electrónico ¿una frontera sin

ley?, es el siguiente: Si estamos hablando con nuestro banco-en el ciberespacio, por supuesto- y deseamos probar nuestra identidad, sólo tenemos que guardar el mensaje con nuestra clave privada (firma); entonces el banco puede abrir el texto con nuestra clave pública, tomada de nuestro certificado digital, lo que prueba que somos la única persona que pudo haber cifrado ese mensaje.

Para el autor chileno Jijena (2002,134) en esencia la firma digital es el sustituto tecnológico de la firma manuscrita u ológrafa, y quien la use, junto con acreditar sin lugar a dudas su identidad, y con la imposibilidad de repudiar después el envío de un mensaje, jurídicamente hablando está manifestando su voluntad en orden a realizar una determinada transacción electrónica con un también determinado cocontratante.

La doctrina ha diferenciado entre los conceptos de firma electrónica y firma digital, los que estarían en relación de género a especie. Firma electrónica sería cualquier código informático que permita determinar la autenticidad del documento y su integridad, y la firma digital una especie de la anterior que resulta de un proceso informático validado e implementado a través de un sistema criptográfico asimétrico de dos claves.

Sin embargo, aún cuando un documento electrónico no este firmado digitalmente, no por ello deja de ser un documento privado cuya declaración no pueda ser imputada a cualquier persona, ya que la firma no es único criterio de imputación. En nuestro derecho la suscripción por sí sola no es suficiente cuando falta el reconocimiento expreso o tácito.

Para hacer valer un documento electrónico como prueba de un hecho o de una transacción o contrato ejecutado por *internet*, la parte debe tomar en cuenta la autenticidad del documento electrónico, su origen y la identidad de la impresión o reproducción con el original

Uno de los medios más eficaces para demostrar que el documento impreso es una copia del original son los sistemas de almacenamiento de datos codificados en un medio *back-up* confiable de una computadora, como lo es un disco óptico.

III. NATURALEZA JURÍDICA DEL DOCUMENTO ESCRITO Y VALOR PROBATORIO.

Considera la autora Sanchis, (1999, 47) que desde un punto de vista exclusivamente físico un documento es una cosa material, mueble, que lleva incorporado un código, un tipo de lenguaje. Es susceptible de aprehensión física y por lo tanto de ser llevado, si ello fuera necesario, a presencia judicial.

El soporte físico del documento ha variado mucho con el paso del tiempo. Históricamente fueron soportes corrientes las tablillas de piedra, arcilla o madera, los papiros y pergaminos, hasta que se llegó al papel. Actualmente, y desde hace ya algunos años, se está dando paso a otro tipo de soportes como los fotográficos, los magnéticos, y más recientemente, los ópticos.

Para Guasp, (1947, 531) la materia de un documento es irrelevante a los efectos procesales, puede venir integrada por cualquier sustancia simple o compuesta, natural o artificial, con tal que su índole no le imponga una imposibilidad de desplazamiento hacia órgano jurisprudencial.

El documento tiene por misión representar, hacer presente algo distinto de sí mismo mediante su evocación. La etimología de la palabra es reveladora puesto que viene de la frase *docere mentem*, declarar o demostrar la intención. Vicente y Cervantes (1856,144 y ss). El documento es, pues, algo que *docet,,* que enseña.

Según Nuñez, (1986, 261,262) lo verdaderamente importante en un documento es su carácter representativo, es decir, la cualidad de actualizar información con relevancia jurídica que ha surgido en un tiempo pasado. El principal rasgo distintivo del documento frente a otros medios de prueba radica en la calidad de esta representación.

Efectivamente y aunque se ha dicho que la reproducción viene a ser en último término cualquier referencia del documento a su contenido y esta referencia se encuentra en todos los medios de prueba, lo cierto es que la representación documental posee una calidad distinta y superior a la del resto de los medios probatorios, fidelidad y perdurabilidad. (Guasp, 1947, 528).

El tema sigue siendo abordado para la autora Sanchis, (1999, 49 y ss) al señalar que el contenido de esa representación es, en sentido amplio,

información con relevancia jurídica. Información relativa a hechos, derechos, estados de cosas o combinaciones entre ellos. El contenido se expresa mediante la utilización de un código. Este código puede ser inmediato o mediato.

Se llama documentos con código inmediato aquellos en los que la información es perceptible directamente por los sentidos, sin ningún intermediario. De tal manera que entre el objeto representador (documento) y la psique humana, no existe nada.

Que podamos o no entender la representación, dependerá de que conozcamos o no el código (por ejemplo sí es un escrito en inglés y no conocemos ese idioma, necesitaremos de un traductor, sí se trata de un plano y no somos arquitectos, necesitaremos de uno para que lo interprete). En todo caso se percibe aparentemente información (ejemplo leemos un informe médico, no entendemos su significado pero entendemos que lo tiene).

La necesidad de concurrencia de la máquina o del traductor humano persiste y deberá ser actualizada cuando la información esté almacenada usando un código desconocido para el receptor. Es decir, que puede repetirse aquí la

misma situación de los documentos con códigos inmediatos pero no conocidos por el destinatario. La diferencia radica en que en los documentos de código mediato siempre necesitaremos una máquina que cumpla la función de hacer que la información almacenada en el documento sea perceptible por nuestros sentidos. La máquina conoce uno o varios lenguajes previos e imprescindibles para acceder a la información. La necesidad del segundo traductor dependerá de nuestro conocimiento o no del código en el que la información se expresa.

Además de los elementos hasta ahora examinados, existen otros dos, la firma y la fecha. Ni una ni otro son elementos fundamentales en los documentos. Es decir, el documento puede existir a pesar de no tener autor conocido ni fecha. Otra cosa será su eficacia jurídica, que se verá sensiblemente mermada por la falta de cualquiera de ellos. Un documento anónimo que no pueda relacionarse con ninguna persona y en el que no conste la fecha, difícilmente tendrá alguna utilidad probatoria a los efectos de un proceso.

En cuanto a la firma dice Serra (1969, 11,19) que en los supuestos en los que la ley no lo exija expresamente como solemnidad esencial del documento, ésta constituirá un elemento muy importante para determinar la

autoría del documento que puede ser acreditada sin embargo de forma distinta, por ejemplo mediante la huella dactilar, que acredita simplemente la presencia de la parte pero no por su autoría, ni el conocimiento de su contenido. O el sello, que se presta a mayores posibilidades de falsificación o de utilización indebida. Un documento privado no firmado ni suscrito puede ser eficaz si es reconocido por su autor.

En lo referente a la fecha, constituye un elemento muy importante sobre todo para establecer sus relaciones de prioridad respecto de otros actos jurídicos.

Con todo lo expuesto, puede expresarse un concepto lógico de documento según el cual "documento es cualquier cosa mueble que represente información con relevancia jurídica relativa a hechos, derechos, estados de cosas o combinaciones entre ellos, mediante un código mediato o inmediato".

Según la doctrina, en cuanto al concepto de documento existen varias posturas, entre ellas la de Montero, quien señala que aunque el proceso civil sea el reino del documento hay que reconocer a continuación que lo paradójico es que no se sabe con exactitud lo que es el documento o por lo menos que desde nuestro derecho positivo no es fácil precisar las fuentes de

prueba que deben incorporarse al proceso por el medio de prueba que se denomina documental. Así pues, no resulta descabellado reconocer que en torno al concepto de documento no hay en la doctrina una posición unánime, sino más bien tres diversas nociones de documento. (1988, 530).

Para Guasp (1988, 530) existe una postura desde la que se concibe al documento con excesiva amplitud como cualquier objeto mueble que dentro del proceso puede ser utilizado como prueba.

Si bien es cierto que la movilidad es una nota común a todos los documentos, no es lo suficientemente individualizadora como para hacer de ella el eje de una concepción del documento, pues aunque todos los documentos son objetos muebles, no todos los objetos muebles son documentos.

Frente a esta concepción amplia existe una posición mucho más restrictiva, que ateniéndose al tenor literal de nuestro Código Civil que identifica el documento, a los efectos procesales, con la prueba por escrito (artículos 1355, 1356 Código Civil). Según los autores que se inscriben en ella, una configuración procesal del documento ajustada a la realidad de nuestro ordenamiento positivo, obliga a calificar como documento únicamente

aquellos objetos que la ley procesal somete al régimen de la prueba documental. De esta manera califica al documento Ortiz, como todo escrito que reproduce un pensamiento una volición humana y se aporta al proceso con designio probatorio. (1994,98).

Desde esa misma posición sostiene Montero, (1988, 145) que el documento es una cosa mueble que representa de modo escrito un hecho o acto jurídico o que es la incorporación de un pensamiento por signos escritos, bien usuales o bien convencionales.(Gómez E. y Herce ,V. 1976, 339)

Existe una postura intermedia que goza en España de más apoyo en la jurisprudencia que en la doctrina y que considera como documento todo objeto material representativo de un hecho de interés para el proceso, representación que puede obtenerse bien mediante el método tradicional de la escritura, bien mediante los modernos medios reproductivos como la fotografía, la cinematografía, el magnetófono, las cintas de video, los discos de ordenador y cualesquiera otros similares.

La concepción de documento como objeto fundamentalmente representador, fue defendida en su momento por Carnelutti, para quien el documento no era sólo una cosa, sino una cosa representativa, o sea capaz de representar un

hecho. De tal modo que la representación de un hecho constituía, a su modo de ver, la nota esencial del concepto de documento. (1982,156).

La ausencia de un documento escrito original firmado por las partes, trae muchos inconvenientes al momento de probar, sobre todo en nuestro país que estamos acostumbrados a la escritura, es decir, la existencia de un documento escrito como base de nuestras transacciones comerciales. Sin embargo, la demostración fehaciente de la identidad de la impresión con el mensaje original se puede lograr a través de la utilización de cualquier medio probatorio.

Efectivamente, nuestro ordenamiento jurídico y específicamente el código de Procedimiento Civil, establece el valor probatorio de los documentos escritos, debido a que la escritura era el único medio de reproducción usual en la época, ello no significa que cualquier avance técnico exija la regulación de un nuevo medio probatorio, y por ello la doctrina y la jurisprudencia deben adaptar dichos nuevos medios reproductivos a las leyes vigentes.

A. EL DOCUMENTO EN SOPORTE PAPEL Y LA FIRMA OLÓGRAFA.

La firma manuscrita tiene validez jurídica en nuestra sociedad y cultura pues en la tradición de su uso se la considera aceptable para identificar al autor de un documento y simultáneamente asegurar la integridad del contenido de ese documento, cuando se cumplen las siguientes condiciones:

1). El documento está escrito con tinta indeleble y en soporte papel absorvente, tal que una enmienda o raspadura que altere la información escrita sea visible y evidente.

2) El documento posee márgenes razonables que contienen los renglones escritos, tal que cualquier escritura adicional sea visible y evidente.

3). La firma manuscrita se coloque delimitando la información escrita, tal que no sea posible agregar texto escrito excepto a continuación de la firma manuscrita.

4). El firmante utiliza siempre la misma o similar firma manuscrita para firmar los documentos de su autoría.

5). La firma manuscrita es suficientemente compleja tal que su falsificación deviene no trivial, y existen peritos caligráficos que pueden detectar las falsificaciones con un razonable

Es importante señalar que la falta de cualquiera de los puntos especificados tornaría inseguro al mecanismo de firma manuscrita para documentos en soporte papel permitiendo así a su autor repudiar la autoría de los documentos que le son atribuidos.

B. DE LA SEGURIDAD DE LA FIRMA OLÓGRAFA Y DE LA FIRMA DIGITAL

La tecnología propuesta de firma digital no es perfecta ni infalible. Los dispositivos en *hardware* y en *software* de creación y verificación de firmas digitales deben ser homologados previa auditoria de su funcionamiento para poder ser utilizados para crear firmas y verificar firmas digitales con plena eficacia jurídica, sin embargo, el requisito de homologación no debe constituirse en una barrera que impida implementar los rápidos avances en el ámbito internacional por lo que se propone que la aprobación tácita de una solicitud de homologación si la autoridad de aplicación no se expide dentro de los 90 días de presentada dicha solicitud.

Por otro lado, es importante destacar que la firma manuscrita tampoco es perfecta o infalible, puesto que es decididamente posible en ciertos casos alterar de forma indetectable el contenido de un documento en soporte papel o falsificar una firma manuscrita. Adicionalmente, debe considerarse que siempre existe un margen de error en la labor de los peritos caligráficos, con lo cual una firma apócrifa puede darse por auténtica y viceversa.

Es usual, por ejemplo, que importantes contratos de compra-venta entre empresas en soporte papel sean firmados por las partes solo en su última página, contando solamente con iniciales en las restantes, lo que a simple vista resulta riesgoso considerando que generalmente el precio establecido en el contrato tiende a no figurar en la última página, sino en alguna página anterior.

Adicionalmente, en *Internet* es de público acceso la información que indica que es técnicamente posible sintonizar un láser para que se corresponda con el color de una tinta, tal que al accionar el láser, la tinta literalmente se vaporiza y se levanta del papel sin dejar rastro detectable alguno.

Sin embargo, las aludidas imperfecciones de los mecanismos de firma manuscrita en documentos en soporte papel no impiden los actos jurídicos, ni gubernamentales ni comerciales que se basan en ella, ni que la firma manuscrita figure como requisito en las leyes y reglamentos de éste país o de otros, por lo que es de inferir que la alternativa propuesta de firma digital de documentos digitales tampoco precisa ser perfecta e infalible para ser de gran utilidad.

Lo importante es la necesidad de gradualismo y proporcionalidad en la especificación de los sistemas y parámetros de firma digital en relación con el tipo de acto en particular, teniendo en consideración las consecuencias jurídicas del acto y/o el valor económico involucrado. De la misma manera que además de requerir soporte papel y firma manuscrita la venta de un inmueble requiere la intervención de un escribano público y la utilización de un protocolo notarial, pero una compra de un electrodoméstico con tarjeta de crédito no, análogamente serán diferentes los requisitos para otorgar validez jurídica a los documentos digitales firmados digitalmente, dependiendo de la naturaleza del acto o de la transacción subyacente.

IV. VALORACIÓN DE LA PRUEBA DEL DOCUMENTO ELECTRÓNICO Y EL DOCUMENTO ESCRITO POR PARTE DE JUECES VENEZOLANOS.

Cuando nos referimos al mensaje de datos como medio de prueba, estamos revisando uno de los temas mas polémicos que existen internacionalmente, no sobre como esos medios de prueba van a ser traídos al proceso sino específicamente la valoración que se le van a dar a esos medios de prueba, particularmente no existe una legislación a nivel internacional que califique específicamente la naturaleza jurídica de esos mensajes.

La Ley sobre Mensaje de Datos y Firma Electrónica sólo establece cual es el valor probatorio que debe otorgársele a esos mensajes, sin embargo no llega a establecer la naturaleza jurídica de esos mensajes, pero lo importante de esta legislación es que se fija la manera se va a valorar ese medio de prueba.

La Ley sobre Mensaje de Datos y Firma Electrónica establece claramente su objeto, el valor jurídico que hay que darle a la firma electrónica, al mensaje de datos y a toda información transmitida por vía electrónica, es decir, que es muy amplio su ámbito de aplicación.

El mensaje de datos comprende toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio, esta definición como podemos observar es muy amplia, pero con base en ella se puede decir que están incluidos lo que son los correos electrónicos, los *web site*, los mensajes lineales (videos, fotografías etc.), todo esto esta contemplado dentro de lo que es un mensaje de datos.

¿El mensaje de datos es igual al documento o se trata de algo distinto?

Inicialmente se señalaba que no se podía comparar el documento electrónico con el documento escrito, el Magistrado Jesús Eduardo Cabrera señalaba que no se podía equiparar el documento electrónico con el documento escrito en papel, porque cuando este mensaje se trasmite utilizando un medio (la computadora) no se puede precisar que la autoría de ese documento le pertenece a la persona, porque a través de la computadora no se puede confiar que esa computadora le transmita al receptor lo que efectivamente le están enviando, con base a este argumento llegó a esa conclusión, pero actualmente se publicó una sentencia en materia de amparo donde quedó establecido la confiabilidad del sistema y menciona las comunicaciones electrónicas, gracias a las revoluciones tecnológicas que han surgido.

En sentencia de fecha 19 de Julio de 2001 con ponencia del Magistrado Jesús Eduardo Cabrera, referida al caso de un amparo constitucional que fue recibido por correo electrónico, y posteriormente ratificado mediante diligencia por los abogados actores. Al respecto consideró la Sala:

> "Esta Sala por interpretación progresiva del artículo 16 de la Ley de Amparo sobre Derechos y Garantías Constitucionales admite que, dentro del medio telegráfico a que hace alusión dicho articulado, está incluido el Internet como medio posible de la interposición de la petición de amparo constitucional, limitándola a casos de urgencia y a su ratificación personal, o mediante apoderado, dentro de los tres días siguientes a su recepción. Ello es así con el fin de no limitar el derecho al acceso a la justicia del accionante, por constituir no sólo un hecho notorio la existencia del Internet como medio novedoso y efectivo de transmisión electrónica de comunicación, además dicho medio se encuentra regulado en el ordenamiento jurídico venezolano por el reciente Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República de Venezuela N° 37.148 del 28 de febrero de 2001, en donde se le da inclusive valor probatorio a dichas transmisiones".

La Ley sobre Mensaje de Datos y Firma Electrónica le atribuye el mismo valor probatorio que tienen los documentos escritos, el artículo 4 dispone: "Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción

y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.

Hay autores como Barriuzo (2000, 207) que analizan los distintos medios de prueba referente a la contratación electrónica y apuntan la posibilidad de adaptar todos y cada uno de ellos a los nuevos soportes

En la prueba documental, se trata de documentos electrónicos representados por cualquier sistema informático, electrónico o telemático cuyo examen estará íntimamente ligado a una pericia de expertos informáticos, por las características del sistema y registro del documento electrónico.

Dentro de estas pruebas la confesión de la parte, se realizará absolviendo posiciones juradas sobre la certeza y veracidad de los documentos generados por procedimientos electrónicos e informáticos aportados y unidos a los autos.

La prueba pericial se hará sobre el contenido y autenticidad del documento electrónico e informático, siempre que tenga influencia en el juicio.

En el reconocimiento judicial se examinarán las instalaciones que han generado el documento electrónico. En caso necesario el Juez, se hará acompañar de un perito para determinar la autenticidad del mismo o el proceso de su elaboración, para determinar posibles manipulaciones.

En el caso de la prueba testimonial consistirá en que personas hábiles, que por cualquier razón hayan estado presentes en el proceso electrónico, o en la generación o manipulación del documento, emitan declaraciones de los hechos observados, con la finalidad de formar la convicción del Juez.

El Decreto con Fuerza de Ley Mensaje de Datos y Firmas Electrónicas señala en el artículo 4 la eficacia probatoria del mensaje de datos concediendo la misma eficacia probatoria que la ley da a los documentos escritos.

La eficacia probatoria de estos documentos, esta íntimamente relacionado con lo establecido en nuestro Código de Procedimiento Civil, en el artículo 429 que regula la prueba instrumental, al señalar que los instrumentos públicos y los privados reconocidos o tenidos legalmente por reconocidos podrán producirse en juicio originales o en copias certificadas y que las copias o reproducciones fotográficas, fotostáticas o por cualquier otro medio mecánico claramente inteligible, de estos instrumentos se tendrán como

fidedignas si no fueron impugnadas por el adversario, ya en la contestación de la demanda si han sido producidas en el libelo, ya dentro de los cinco días siguientes si se han producido después de la contestación o en el lapso probatorio y las que hubieren sido producidas en otra oportunidad no tendrán ningún valor probatorio si no son aceptadas expresamente por la otra parte.

En cuanto a los medios de prueba, nuestro Código de Procedimiento Civil, señala en el artículo 395 los medios de prueba admisible, asumiendo que tenemos medios de pruebas libres al establecer:

> "(...) Son medios de prueba admisible en juicio, aquellos que determine el Código Civil, el presente Código y otras leyes de la República.
> Pueden también las partes valerse de cualquier otro medio de prueba no prohibido expresamente por la ley, y que consideren conducentes a la demostración de sus pretensiones. Estos medios se promoverán y evacuarán aplicando por analogía las disposiciones relativas a los medios de prueba semejantes contemplados en el Código Civil, y en su defecto en la forma que señale el Juez.(...)."

Según lo señalado anteriormente, en nuestro país la demostración plena de la identidad de la impresión y la autenticidad del mensaje o registro electrónico con el original, así como su origen se puede lograr a través de cualquier medio de prueba. El problema se presenta al tratar de buscar la vía

más adecuada a través de la cual se hayan de introducir las pruebas en el proceso.

La información contenida en un mensaje de datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas, esa discusión teórica sobre si se debe equiparar el documento escrito con el documento electrónico ya queda un poco estéril por la valoración que le van a dar a estos mensajes de datos en un proceso judicial.

Es muy importante saber, cual es el valor probatorio que se le deben dar a esas impresiones que se hacen de los mensajes de datos, esas impresiones pueden ser consideradas como una fotocopia y si no son desconocidas por la otra parte se tienen como bien presentadas, atribuyéndose en consecuencia el mismo valor probatorio que se le da a la fotocopia.

El Dr. Arístides Rengel Romberg ha considerado que si esta impresión no es desconocida por la otra parte tiene valor probatorio, es el mismo que se le da a la fotocopia si esta se acompaña con el libelo de demanda y si no es desconocida por la otra parte, se considera que ha sido reconocida y por lo

tanto tiene el valor probatorio como si se hubiera acompañado un documento escrito.

Esta posición no es compartida por otros autores, dentro de los cuales encontramos al Magistrado Jesús Eduardo Cabrera, quien considera que en el caso de documentos informáticos, es necesario por la misma facilidad con la que se pueden obtener esos mensajes que se acompañen otros medios de prueba que garanticen la integridad de los mismos, es decir, que el mensaje es el mismo que fue transmitido o que al menos nos de unas presunciones suficientes para llegar a esa conclusión y así otros mecanismos de prueba adicionales que no se limitan simplemente a la consignación de una fotocopia.

Podría aplicarse el reconocimiento tácito al documento si no es desconocido por la otra parte, tal como lo dispone el Código de Procedimiento Civil, el Juez al momento de entrar al análisis probatorio para determinar el valor probatorio de ese documento entonces tendrá que considerar todos los elementos adicionales antes de llegar a una valoración definitiva independientemente de lo que dice el documento del mensaje de datos electrónico, pero esto es solamente en lo que se refiere a la fotocopia.

Hay otras formas de traer el mensaje de datos al proceso. El artículo 8 de la Ley sobre Mensaje de datos y Firma Electrónica establece:

> "Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta. Cuando la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los Mensajes de Datos, siempre que se cumplan las siguientes condiciones:
> 1. Que la información que contengan pueda ser consultada posteriormente.
> 2. Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.
> 3. Que se conserve todo dato que permita determinar el origen y el destino del Mensaje de Datos, la fecha y la hora en que fue enviado o recibido.
> Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo."

El mensaje de datos debe conservarse tal y como dispone el artículo precedente, asimismo se establecen una serie de requisitos para dar cumplimiento a dicho archivo de datos. En las notarias, los registros, los tribunales, todos podrían llevar un archivo electrónico de todos los documentos que se van presentando ante las autoridades, estamos en consecuencia acercándonos más a una equivalencia entre los documentos escritos y los documentos electrónicos y adicionalmente vemos que también

la ley establece que el documento debe cumplir ciertas solemnidades, referidas al otorgamiento, las cuales se deben cumplir a través del mensaje de datos, como por ejemplo: aquellos documentos donde se requiera la firma, que esta cumpla con esos requisitos que dice expresamente la ley, cuando se requiere incluso que se conserve el documento original, pero aun así no podemos hablar de una equivalencia absoluta.

La Ley sobre Mensaje de Datos y Firma Electrónica establece claramente como debe manejarse esta promoción y evacuación de las pruebas, asimismo dispone que pueden ser traídos al proceso todos los medios de prueba que nos permiten recabar toda la información contenida en el documento, no solamente la producción del documento como tal sino valerse de todos los medios de prueba que facilitan esa traída del documento al proceso.

En cuanto a la producción de la fotocopia solamente se limita a los documentos que cumplen ciertas características:

1) Documentos públicos o privados reconocidos.

2) Que sean producidos en el lapso probatorio

3) Que no hayan sido impugnados por la otra parte

4). Que sean claramente legibles

Si no se cumple con estos requisitos no se pueden traer al proceso como una impresión, sino que deben llevarse al proceso mediante otro medio de prueba.

Cuando nos referimos a un documento público, sabemos que lo que hace que un documento sea público no es el mecanismo que hemos utilizado para otorgarlo, sino la participación de un funcionario revestido de fe pública.

A.- PROMOCIÓN Y EVACUACIÓN DEL MENSAJE DE DATOS Y LA FIRMA ELECTRÓNICA EN EL PROCESO.

Los medios de prueba que se pueden utilizar para traer esos mensajes de datos al proceso son: en primer lugar la inspección judicial, esta inspección judicial debe cumplir con el requisitos de traer el documento electrónico al proceso y debe ser practicada en un lugar donde exista un proveedor de conexión a la *Internet* a los fines de ofrecer mayor seguridad de su contenido.

¿Que valor probatorio se le va a dar a esa inspección judicial?

La Ley sobre Mensaje de Datos y Firma Electrónica establece que el valor probatorio que se le debe dar al mensaje de datos es el mismo valor

probatorio que se le da al documento escrito, pero eso no quiere decir que si se promovieron los mensajes de datos al proceso a través de una inspección judicial se le tenga que dar el valor probatorio del documento escrito, sino que la inspección judicial se complementa con otra serie de pruebas que lleguen a demostrar la autoría, el lugar de emisión, el momento, todo eso por el principio de la comunidad de prueba ayudaría a darle a ese mensaje de datos el valor probatorio de un documento, allí si se cumpliría el principio establecido en la ley.

Debe ser verificado el autor, el momento de realización del mensaje, la integridad del mensaje, esto tiene una clave mucho mas tecnológica puesto que había que demostrarle al Juez que el mecanismo que se utilizó para la trascripción del mensaje es el que nos permite que el mensaje de datos no sea alterado, que sería el caso de las firmas electrónicas certificadas que ese mecanismos permite certificar que ese mensaje de datos no fue alterado, es integro, teniendo esto como una presunción *iuris tantum*, toda vez que el principio de unidad o comunidad de la prueba ofrece más garantías.

En segundo lugar tenemos a la prueba de informes; mediante esta prueba se le puede requerir a un tribunal, un notario o un registrador que nos emita un informe sobre los mensajes de datos que tienen almacenados en su servidor.

Las partes pueden facilitar la valoración promoción y evacuación de los documentos en el proceso cuando han firmado por ejemplo un contrato en el cual se establece que todos los documentos que lleguen a su servidor en un determinado correo electrónico o un mecanismo determinado de criptografía, entonces le corresponderá al Juez verificar el cumplimiento de lo estipulado en dicho convenio, haciendo de este modo más fácil la valoración de dichas pruebas.

B. LA VALORACIÓN DE LOS DOCUMENTOS ELECTRÓNICOS.

Acogiéndonos a la definición amplia del documento, como cosas muebles aptas para la incorporación de señales expresivas de un determinado significado, debemos concluir que los registros o soportes electrónicos constituyen verdaderos documentos, pues en ellos, se recogen expresiones del pensamiento humano o de un hecho incorporándolos a su contenido, que es lo que los hace capaces de acreditar la realidad de determinados hechos.

1. La prueba de los hechos

El documento electrónico puede contener información escrita, pero a diferencia de la escritura tradicional, el mensaje de datos en él contenido no

puede ser leído por el hombre sin el auxilio del computador, que fungiría de decodificador.

Considera el autor Jijena que en la legislación comparada o en el derecho extranjero, nada obsta a que las partes intervinientes en un intercambio electrónico de documentos generen, y los tribunales acepten como prueba, el registro magnético de la operación, otorgándole el mismo valor que tendría un documento escrito, no obstante que las firman del emisor y del receptor sean claves digitales o electrónicas. En el evento de un litigio, los tribunales no tienen inconveniente en admitirle mérito probatorio, por cuanto su sistema lo rige el denominado "principio del libre convencimiento, de la prueba libre o de la persuasión racional del juez en la valoración de las pruebas. Así ocurre en sistemas procesales como el italiano o el argentino (2002, 163).

Al hablar del valor probatorio del documento electrónico, se esta haciendo referencia a las pruebas pertinentes o a la adecuación que deben tener las pruebas con el tema u objeto del juicio. Lo que interesa y da validez a las pruebas empleadas es la relación que las pruebas guardan con lo que constituye el tema *decidendum* para el tribunal y expresa la capacidad de los medios utilizados para formar la definitiva convicción del Tribunal.

Analizando los medios de prueba y siguiendo nuestro Código de Procedimiento Civil en consonancia con las nuevas tecnologías y los caracteres generados por las mismas, podemos decir:

a) Por instrumentos o documentos electrónicos, entendemos el soporte o el medio, donde queda constancia de los datos, el proceso, de los resultados, o de las decisiones de un sistema electrónico, informático o telemático de cualquier tipo.

b) Por confesión de las partes, sobre la certeza y veracidad de los documentos generados por procedimientos electrónicos e informáticos aportados y unidos a los autos.

c) Por prueba pericial del documento generado por procedimiento electrónico e informático, sobre su contenido y autenticidad, que sea de influencia en el pleito; designando el documento electrónico o la cosa que ha de ser objeto de pericia y señalando en que consistirá la pericia o si han de ser uno o tres los peritos para llevarlo a efecto.

Como prueba de autenticidad de algún documento o registro electrónico pueden valer las encriptaciones, codificaciones, claves o también los

registros internos generados por el reloj del sistema, por *reports* automáticos, configuraciones etc. El experto en ordenadores, facilitará la determinación del objeto de la pericia y su presentación.

d) Por reconocimiento judicial, de las instalaciones que han generado el documento electrónico o informático, para determinar la autenticidad del mismo o el proceso de su elaboración, y posibles manipulaciones.
e) Por testigos, es decir, personas hábiles que por cualquier razón hayan estado presentes en el proceso electrónico o en la generación o manipulación del documento.

El profesor Guasp define al testigo, como una tercera que, sin ser parte en el proceso, emite declaraciones sobre datos que no habían adquirido índole procesal para el declarante en el momento de su observación, con la finalidad de formar la convicción del juez en un determinado sentido (1977,144).

Remarcando el carácter no exhaustivo de la enumeración de medios probatorios por parte de nuestro Código de Procedimiento Civil, podemos decir, que las innovaciones tecnológicas, videos, cintas magnetofónicas, ordenadores electrónicos, etc. pueden y deben incorporarse al acervo

jurídico procesal en la medida en que son expresiones de la realidad social que el derecho no puede desconocer. Dichos medios pueden subsumirse en el concepto de documento, en cuanto cosas muebles aptas para la incorporación de señales expresivas de un determinado significado. No existen sin embargo, normas especificas sobre los criterios a seguir y requisitos exigibles para la práctica de estos medios, resultando necesaria una regulación sobre la forma de realizarse.

La Jurisprudencia española sobre este punto señala que el artículo 575 LEC y el 1215 del C.C, enumera los medios de prueba, no los valora por su orden, y las partes pueden elegir los medios que estimen oportunos, dando valor al principio dispositivo de las partes.

El derecho a utilizar los medios de prueba pertinentes para la defensa, en aquellos casos en que la prueba está representada por los soportes informáticos y cuando la prueba es inadmitida conlleva la vulneración del derecho a la defensa.

Al examinar la jurisprudencia constitucional española, se observa que existe en primer lugar el derecho a proponer la prueba, luego el derecho a que la prueba pertinente sea admitida y en caso de no serlo, a una inadmisiòn

motivada, razonable y no arbitraria, y en tercer lugar el derecho a practicar la prueba admitida. Junto a todo ello será necesario, para poder estimar el recurso de amparo por lesión del derecho, que la vulneración producida haya causado indefensión a la parte recurrente.

En palabras del propio Tribunal constitucional el contenido del derecho a utilizar los medios de pruebas pertinentes es inseparable del derecho mismo a la defensa y consiste en que las pruebas pertinentes propuestas sean admitidas y practicadas por el Juez o Tribunal (sent. 20 de febrero de 1996).

2. La prueba de los contratos electrónicos

En nuestra legislación en primer lugar, debemos considerar que el original de un mensaje o correo electrónico o de cualquier registro telemático es el que circula por la red y que puede ser leído a través del computador, por ello lo que se ofrecerá como prueba y se presentará en el expediente judicial es el documento electrónico archivado en un disquete o su impresión.

La parte promovente deberá afirmar y probar como medio probatorio atípico o innominado, las circunstancias que convenzan al Juez de que la impresión o el registro contenido en el disquete es una representación genuina de su

original. Ahora bien, esa prueba promovida debe ser una prueba pertinente para que pueda ser admitida por el Tribunal.

Para la autora Sanchis (1999, 31) las características de una prueba para que pueda ser considerada pertinente, son:

1).- Que el objeto de la prueba sean hechos y no normas jurídicas o elementos de derecho

2).-Que los hechos estén previamente alegados, y por tanto, aportados al proceso.

3).- Que no se trate de hechos exonerados de prueba.

La apreciación de la pertinencia o no de la prueba propuesta corresponde al órgano jurisdiccional, y en caso de declararla impertinente deberá hacer un auto motivado y razonado el cual puede ser apelado por la parte y su apelación se oirá en un solo efecto.

Montero (1998, 76,77) se refiere a la posibilidad material de que se practique el medio de prueba diciendo que es un aspecto complementario de la legalidad de la actividad probatoria para la que hay que atender, a que exista realmente la fuente de prueba y que la misma pueda incorporarse al proceso Si se propone, un medio de prueba respecto de una fuente que, por la causa que sea, o ya no existe, o jamás existió, o bien existe pero es de muy difícil

consecución, no tendrá sentido preguntarse si el hecho que se pretende probar con ella, es o no pertinente Vg. una fuente de prueba destruida completamente en un incendio o situada en un país en guerra, por supuesto no será admitida, porque no se podrá realizar la práctica de la misma.

El profesor Cabrera Romero ha señalado que sobre la credibilidad del medio desde el punto de vista del Juez cubre dos aspectos: uno concreto, consistente en la verosimilitud del medio como aportador de algo serio, y otro abstracto relacionado con el convencimiento interno del Juez sobre la conductibilidad del medio, esto es si es capaz de trasladar al proceso los hechos controvertidos (1989, 237).

Con un criterio contrario, se presenta el Dr. Arístides Rengel Romberg, quien señala que "no es la oportunidad de la promoción de la prueba, la prevista para desembarazarse de la carga de probar la autenticidad y la credibilidad del documento, sin necesidad de la actividad de la contraparte, sino en la incidencia provocada por el desconocimiento del documento, pues en caso de silencio de la parte contra la cual se produce el documento, éste queda reconocido" y añade que "Es generalmente admitido en doctrina, que un control preventivo de la relevancia o idoneidad de la prueba documental del tipo de las reproducciones mecánicas y pruebas científicas, no puede

realizarlo el Juez en la etapa de admisión de la prueba, sino que pertenece a la apreciación de su eficacia, después de su adquisición".

La opinión del Dr. Rengel Romberg, mantiene un criterio de muy avanzada percepción, sin embargo el criterio del Dr. Cabrera Romero, merece igualmente mucha importancia al mencionar que el silencio de la parte sobre los datos y su prueba, puede obrar contra él mismo, pues al no cumplir con el requisito de la eficacia probatoria, correrá el riesgo de que el Juez no valore la prueba en la sentencia definitiva.

En conclusión para que la prueba de un documento electrónico, tenga eficacia probatoria debe ser necesario que el promovente demuestre la autenticidad y para ello será necesario que se compruebe el origen, la identidad del documento original con el impreso y finalmente su autoría.

Es decir, que los diferentes elementos que componen el sistema electrónico de la informática pueden ser presentados como prueba en cuanto fuesen pertinentes para acreditar los hechos controvertidos. En definitiva la eficacia de su fuerza de convicción está supeditada a la prudente y sana critica del Juez, pudiendo éste auxiliarse con peritajes de expertos, consultas científicas o técnica y otros medios de prueba.

3. El desconocimiento de la prueba documental electrónica

Cuando los litigantes contradicen las alegaciones y las pruebas, entramos en el principio del contradictorio o de audiencia bilateral. El principio del contradictorio es una de las manifestaciones del derecho a la defensa, pues ello significa que se oye a la s partes respecto de las actuaciones llevadas a cabo por la contraria.

Cuando la parte pretenda valerse del documento electrónico y demuestra en juicio la autenticidad y autoría del mensaje o registro contenido en un disquete o en un papela impreso, ello no impide que su contraparte trate de impugnar su eficacia y validez como medio de prueba.

En caso de producirse el desconocimiento del documento electrónico el Juez o el árbitro, deberán adaptar el procedimiento tradicional contenido en el Código Procedimiento Civil para la prueba instrumental.

El promoverte de la prueba electrónica deberá demostrar que el mensaje se envió desde la computadora de su contraparte o que la firma digital contenida en el documento le pertenece efectivamente.

4. Jurisprudencia del Tribunal Supremo de Justicia

Resulta imposible no aceptar, en la actualidad que los jueces a través de sus sentencias crean derecho, lo cual es una consecuencia que con el paso del tiempo han acercado sus sentencias a la realidad social que vive un país, por eso las sentencias de los tribunales de un país, se constituyen en fuentes inagotables para el estudio del derecho y de cualquier tema, en especial, el referente al valor probatorio de la firma electrónica y el mensaje de datos, el cual ha sido desarrollado principalmente a la luz de la jurisprudencia, toda vez que no se previó de manera especifica su tratamiento en el Decreto con Fuerza de Ley Mensaje de Datos y Firmas electrónicas

La Jurisprudencia ha sido definida, como aquella doctrina que reiteradamente se presente en las sentencias, lo cual por lo general se circunscribe en un lapso de tiempo, en el cual tiene vigencia siempre y cuando se adecue a la necesidad del colectivo que es en definitiva el destinatario de la ley que en principio le da vida.

El tema del valor probatorio de la firma electrónica y el mensaje de datos, es novedoso, ello explica el porque no son abundantes los fallos sobre el tema.

No. 01-2001 Sentencia de la Sala Constitucional, fecha: 19 de Julio 2001. Causa: Leonardo Pérez en Amparo Constitucional

Refiere al caso de un amparo constitucional que fue recibido por correo electrónico, y posteriormente ratificado mediante diligencia por los abogados actores. Al respecto consideró la Sala:

> "Esta Sala por interpretación progresiva del artículo 16 de la Ley de Amparo sobre Derechos y Garantías Constitucionales admite que, dentro del medio telegráfico a que hace alusión dicho articulado, está incluido el Internet como medio posible de la interposición de la petición de Amparo Constitucional, limitándola a casos de urgencia y a su ratificación personal, o mediante apoderado, dentro de los tres días siguientes a su recepción. Ello es así con el fin de no limitar el derecho de acceso a la justicia del accionante, por constituir no sólo un hecho notorio la existencia de Internet como medio novedoso y efectivo de transmisión electrónica de comunicación, además dicho medio se encuentra regulado en el ordenamiento jurídico venezolano por el reciente Decreto ley sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República de Venezuela Nº 37.148 del 28 de febrero de 2001, en donde se le da inclusive valor probatorio a dichas transmisiones"

En el presente caso, se interpone un amparo constitucional utilizando la vía de Internet y posteriormente los actores del amparo ratifican el mismo. Con ello se facilita el acceso a la justicia, lo que constituye un avance en nuestro ordenamiento jurídico.

No 02-2001.Sala Constitucional. Sentencia 3 agosto 2001.Causa: Gerardo Ortiz Rey. Amparo Constitucional.

Amparo intentado por violación al derecho a la defensa al debido proceso, al derecho de propiedad y dedicarse a actividad económica de su preferencia.

> "La Sala no puede obviar que el sitio Web de este Máximo Tribunal ha sido concebido como un medio auxiliar de divulgación de su actividad judicial cuya finalidad es permitir el acceso de todos los ciudadanos a la administración de justicia, especialmente aquellas personas que como el demandante viven en el interior de la república, finalidad que expresa este Máximo Tribunal al transcribir al pie de la presentación de la pantalla del sitio Web, el contenido del artículo 26 de la Constitución de la República Bolivariana de Venezuela, todo lo cual permite al público inferir lícitamente que la información que contiene, si bien no es merecedora de fe pública, si es fiel reflejo de las actuaciones del Máximo Tribunal y no hay en la página alguna advertencia que desvirtúe tal conclusión por de más lógica por parte del público usuario. De allí que esta Sala considere, que aún cuando las cuentas publicadas en el sitio web no cumplen a cabalidad con los requisitos para hacer fe de las menciones que contienen, se presentan ante el público usuario de tal manera que les hace merecedora de confianza y no puede este tribunal ignorar esta situación"

El presente caso se refiere al hecho de que no apareció en la cuenta de la Sala Nº 107, la información referente a que se celebraría el acto de la audiencia constitucional, razón por la que el accionante no acudió a la misma, a pesar de que la información publicada en el sitio web era absolutamente confiable y a través de ella se había enterado de todas las incidencias del proceso, por lo que era razonable confiar en que la fijación de la audiencia constitucional también aparecería publicada en las cuentas.

Sentencia Nº 03-2001. Sala Constitucional. Sentencia: 9 de marzo 2001. Causa: Oswaldo Alvarez. Amparo Constitucional.

Trata el presente caso el correo electrónico dirigido en fecha 9 de julio de 2000 a la página Web de *internet* del Tribunal Supremo de Justicia, por el ciudadano Oswaldo Álvarez, titular de la cédula de identidad número 4.454.621, actuando en su propio nombre, mediante el cual ejerció acción de amparo constitucional por la omisión de pronunciamiento respecto a dos expedientes que cursan ante ese Alto Tribunal, siendo el primero de ellos llevado ante la Sala Político Administrativa bajo el número 13.765 y el segundo, llevado ante la Sala Plena bajo el número 843, por la supuesta violación de su derecho de petición.

"La Sala para decidir observa:

> Esta Sala por interpretación progresiva del artículo 16 de la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales admite que, dentro del medio telegráfico a que hace alusión dicho articulado, está incluido el *Internet* como medio posible de interposición de la petición de amparo constitucional, limitándola a casos de urgencia y a su ratificación, personal o mediante apoderado, dentro de los tres (3) días siguientes a su recepción. Ello es así con el fin de no limitar el derecho al acceso a la justicia del accionante, por constituir no sólo un hecho notorio la existencia del Internet como medio novedoso y efectivo de transmisión electrónica de comunicación, sino que, además, dicho medio se encuentra regulado en el ordenamiento jurídico venezolano por el reciente Decreto Ley Nº 1204 sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República de Venezuela Nº 37.148 del 28 de febrero de 2001, en donde se le da inclusive valor probatorio a dichas transmisiones.

Ahora bien, reza el artículo 16 de la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales:

"La acción de amparo es gratuita por excelencia. Para su tramitación no se empleará papel sellado ni estampillas y en caso de urgencia podrá interponerse por vía telegráfica. De ser así, deberá ser ratificada personalmente o mediante apoderado dentro de los tres (3) días siguientes. También procede su ejercicio en forma verbal y, en tal caso, el Juez deberá recogerla en un acta" (subrayado añadido).

Ahora bien, visto que no consta en autos que la acción de amparo a que se ha hecho referencia y que fuere interpuesta por vía de *internet* haya sido ratificada en la forma prevista en la norma *supra* transcrita, ni tempestivamente ni fuera del lapso prescrito al efecto, la precitada solicitud debe declararse inadmisible, y así se decide".

.V. LA FIRMA ELECTRONICA EN EL DERECHO COMPARADO.

Nuestra legislación esta inspirada en la comunitaria, de ahí que en el derecho comparado se haya incluido la Directiva 1999/93 CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica.

También en materia de firma electrónica nos parece necesario incluir legislación de países como España, Argentina, Chile, Alemania y por supuesto la Ley Modelo sobre Comercio Electrónico aprobada por las Naciones Unidas para el Derecho Mercantil Internacional.

A.- FIRMA Y DOCUMENTOS DIGITALES O ELECTRONICOS EN EL AMBITO DE ORGANISMOS INTERNACIONALES Y DEL DERECHO COMPARADO.

Por la importancia que presentan toca analizar el contenido de las Leyes Marco de la UNCITRAL y la Unión Europea y sobre la Ley aprobada para España teniendo en cuenta que se trata de temas muy recientes mundialmente y por tanto no existe consensuada estandarización jurídica acerca de cómo debe regularse el tema de la prestación de servicios de certificación digital y el uso de firmas electrónicas o digitales.

Sin embargo, en América Latina hemos tenido un proceso de fecundidad legislativa. Argentina, Colombia, Perú, Venezuela, Panamá y Chile ya cuentan con leyes de firma digital y/o electrónica, con inconveniente, porque se trata de normas casi en abstracto, ya que en la mayoría de estos países no existen prestadores de servicios de certificación local operando y todas ellas han caminado de la mano de la estandarización normativa que reclama la creciente globalización de las economías y de las sociedades modernas.

1. LEYES MODELOS DE LA CNUDMI (COMISION DE NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL O UNCITRAL), Y DOCUMENTOS DE TRABAJO SOBRE COMERCIO ELECTRONICO Y FIRMA DIGITAL.-

La Asamblea General de la ONU, mediante Resolución 51/162, de 1996, aprobó la Ley Modelo Sobre Comercio Electrónico, elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, o CNUDMI, y recomendó su incorporación a los ordenamientos internos como un instrumento útil para agilizar las relaciones jurídicas entre particulares, siendo esta un primer antecedente obligado para el estudio de la regulación jurídica del *e-commerce,* tiene la finalidad de servir de referencia a los países en la evolución y modernización de ciertos aspectos de sus leyes y

practicas en las comunicaciones con medios computarizados y otras técnicas modernas y en la promulgación de la legislación pertinente cuando no exista legislación de este tipo.

Pero esta Ley Modelo de la UNCISTRAL, sobre Comercio Electrónico, analizó el tema de de las firmas y comercios electrónicos sin mencionar las firmas digitales o la criptografía, manteniendo un criterio de neutralidad tecnológica. Su artículo 7° señala que cuando la ley exija la firma de personas, esta exigencia se entenderá cumplida, a propósito de un mensaje electrónico firmado, si se utiliza un método (cualquiera que sea) para identificar a las personas intervinientes y para indicar la aprobación por parte de ellas de la información o del documento contenido en un mensaje electrónico.

En el año 1997, concretamente en el mes de mayo, se encomendó al grupo de trabajo sobre Comercio Electrónico la preparación de un informe sobre los aspectos jurídicos que plantean las firmas numéricas y las entidades certificadoras. Con respecto a la forma y al alcance de ese régimen uniforme, en ese período de sesiones se acordó que en esa etapa aún no podían adoptarse decisiones y se consideró, que el Grupo de Trabajo centrara su atención en problemas que plantearan las firmas numéricas ante la evidente

preponderancia de la criptografía de clave pública en las nuevas prácticas de comercio electrónico, que el régimen uniforme que se preparara debía ajustarse al criterio de neutralidad que se había ajustado previamente en la Ley Modelo de CNUDMI sobre Comercio Electrónico.

Señala el autor Jijena que el régimen uniforme no debería desalentar la utilización de otras técnicas de autenticación, y que al regularse la criptografía de clave pública convendría que el régimen uniforme previera diversos grados de seguridad y reconociera los diversos efectos jurídicos y los gastos de responsabilidad que se derivaran de los servicios prestados en el contexto de las firmas numéricas. Con respecto a las entidades certificadoras, consideró que seria conveniente que el Grupo de Trabajo previera el establecimiento de una serie mínima de normas que hubieran de cumplir las entidades certificadoras (2002,186).

Fruto de ese trabajo, a fines de 1998 y comienzos de 1999 se han liberado dos documentos sobre régimen uniforme para las firmas digitales y las entidades certificadoras, ordenamiento –marco- que, no obstante reconocer la importancia de los sistemas de criptografía asimétrica o de dos llaves, también mantiene un criterio de neutralidad tecnológica para no desalentar el uso de otras tecnologías de autenticación y establece criterios comunes

respecto del régimen legal de las firmas digitales para lograr que exista una infraestructura internacional para el comercio electrónico.

Estas normas pueden constituir, en opinión de UNCITRAL, o un ordenamiento jurídico separado o ser incorporadas a una ley marco sobre comercio electrónico. La finalidad de estos documentos, fue la de promover una utilización eficaz de las comunicaciones digitales estableciendo un marco de seguridad y dando a los mensajes digitales un estatuto jurídico igual al de los documentos soportados en papel.

El paso siguiente fue abocarse, durante 1999 y el año 2000, a la redacción de un régimen uniforme y articulado que sirviera como Ley Modelo a los países miembros.

La finalidad de que exista un régimen uniforme, al decir de la Secretaría de la UNCITRAL, es la de facilitar el creciente empleo que se hace de las firmas electrónicas en las operaciones comerciales internacionales. Inspirándose en los instrumentos legales ya en vigor o que se estaban preparando en algunos países, se buscó en la CNDUDMI prevenir una eventual falta de armonía en el régimen aplicable al comercio electrónico sentando -para lograrlo- una serie de pautas para que se reconozca la validez jurídica de las firmas

electrónicas, con la asistencia eventual de entidades certificadoras, para las cuales se consideraron un cierto número de reglas básicas.

Al haberse adoptado como base la Ley Modelo-señala la Secretaría de la UNCITRAL-, el régimen uniforme trata de reflejar el principio de la neutralidad respecto de los medios técnicos utilizados; el criterio de la no-discriminación de todo equivalente funcional de los conceptos y prácticas que tradicionalmente funcionan sobre soporte de papel; y una amplia confianza en la autonomía contractual de las partes.

El proyecto de régimen uniforme fue concebido, por último, para ser usado como marco normativo mínimo en un entorno abierto, como el de la red Internet (es decir, un ámbito en el que las partes negocien por vía electrónica sin acuerdo previo, inquietud que a su turno había sido compartida por la Directiva de la Unión Europea, y como reglas de derecho supletorio para un entorno cerrado es decir, ámbito en el que las partes estén obligadas por reglas contractuales y procedimientos previamente estipulados para negociar por vía electrónica.

Fue en la 38ª sesión de la UNCITRAL, realizada en marzo de 2001 en Nueva York, cuando se aprobó un proyecto detallado de guía para la incorporación al derecho interno de cada país de la Ley Modelo.

Los capítulos más relevantes del régimen uniforme propuesto como Ley Modelo de Firma Digital debida y sistemáticamente estructurados en 12 artículos se refieren a las firmas digitales, a sus definiciones y requisitos jurídicos, establecen presunciones de autoría e integridad, aluden al contenido de los certificados, a las entidades certificadoras y sus responsabilidades, y a la revocación, suspensión y registro de los certificados. Son, por cierto, los aspectos mínimos que debe contener toda ley sobre firmas y documentos digitales o electrónicos.

El artículo 1º se refiere a su ámbito de aplicación, esto es, por regla general a todos los casos en que se utilicen firmas electrónicas en el contexto de actividades comerciales tales como el suministro e intercambio de bienes comerciales, sin que esté derogando o deba derogarse norma alguna destinada a la protección del consumidor.

El artículo 2º contiene una serie de definiciones esenciales. Por firma electrónica se entiende "al conjunto de datos en forma electrónica

consignados en un mensaje de datos-léase documento-, o adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba hay una manifestación de voluntad la información contenida en el mensaje de datos."

Por certificado en estricto rigor de identidad más que de una firma electrónica específica- se entiende todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma.
Por mensaje de datos, considerando tanto el contenido como el continente, se entiende la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o similares, como pudieran ser , entre otros, el intercambio electrónico de datos, el correo electrónico , el telegrama, el télex o el telefax.

Por prestador de servicios de certificación se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

El artículo 3º se refiere a la igualdad en el tratamiento de la tecnología para las firmas electrónicas o a la tan comentada neutralidad tecnológica,

señalando que, salvo común acuerdo de las partes, las disposiciones legales no podrán ser aplicadas de modo que se excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumplan con los requisitos que las leyes establezcan.

El artículo 6 establece como se cumple con el requisito de idoneidad de una firma electrónica atribuida a una persona, y en relación con un mensaje de datos, a saber, ampliamente y en consideración a sus efectos, cuando a la luz de todas las circunstancias del caso sea fiable y resulte apropiada a los fines para los cuales se generó o comunicó el mensaje. Agrega en uno de sus incisos la descripción de diversos casos en que una firma electrónica se considerará fiable, esto es cuando los datos de creación de la firma correspondan contextual y exclusivamente o hayan estado en el momento de la firma bajo el control exclusivo del firmante, cuando sea posible detectar cualquier alteración de la firma electrónica o de la integridad de la información contenida en el mensaje y/o documento realizada con posterioridad a su generación.

Los artículos 8º, 9º, 10 y 11 de la Ley Modelo aluden al proceder del firmante o signatario, o de los prestadores de servicio de certificación y de los terceros que confían en los certificados digitales a efectos de poder utilizarse datos de

creación de firmas o prestarse servicios de apoyo para obtener como resultado del proceso tecnológico firmas con efectos jurídicos.

El firmante deberá actuar con diligencia razonable para evitar el uso no autorizado de sus datos de creación de firmas (Vg. para que no se conozca su clave privada), avisar sin dilación indebida cuando crea que su firma carece de fiabilidad, y verificar la exactitud y cabalidad de los datos que contenga un certificado que lo respalde.

2. DIRECTIVA SOBRE FIRMA DIGITAL DEL PARLAMENTO EUROPEO Y DEL CONSEJO, PROPUESTA EL 13 DE MAYO DE 1998 Y APROBADA EL 13 DE DICIEMBRE DE 1999 (DIRECTIVA 1999/93/CE)

A través de esta Directiva se estableció un marco comunitario para la firma electrónica.

Las soluciones propuestas son esencialmente válidas para el ámbito de la Comunidad Europea, en el que no existen fronteras ni barreras arancelarias, donde poseen una moneda común y donde en definitiva funcionan como un solo mercado de transacciones, por lo que no son directamente aplicables a realidades como el mercado venezolano.

Frente al problema de la seguridad de las comunicaciones electrónicas en la Unión Europea, se constató la existencia de diversas iniciativas locales y, por ende, la necesidad de adoptar un marco legal común, armonizado u homogéneo para regular y reconocer el uso y los servicios de certificación de firmas digitales, solamente tratándose de redes abiertas como Internet y de forma neutral desde el punto de vista tecnológico, es decir, sin inclinarse en la directiva por algún sistema de firma digital determinado, como por ejemplo podría ser la criptografía de clave pública.

La Directiva consta de un preámbulo, que explica las razones del texto propuesto, en especial, que a la hora de estamparse firmas digitales se requiere la necesidad de establecer un sistema de proveedores de servicios de certificación amplio, de 15 artículos y de dos anexos relacionados con dos importantes elementos jurídicos: uno, sobre requisitos de los certificados reconocidos y otro, sobre los requisitos a satisfacer por los proveedores de servicios de certificación.

Según lo estipulado en la Directiva, se buscó facilitar el uso de la firma electrónica en un espacio sin fronteras interiores y eliminar obstáculos, concretamente las diferencias en el reconocimiento legal de la firma

electrónica y las restricciones al libre movimiento de servicios y producto de certificación entre los Estados miembros.

El considerando sexto de la Directiva, señala que los rápidos avances tecnológicos y la dimensión mundial de *internet* precisan un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos, no obstante que la firma digital basada en la criptografía de llave pública constituía a esa fecha y constituye actualmente la forma más reconocida de firma electrónica.

El artículo 2º define el concepto de firma electrónica como la firma en forma digital integrada en unos datos, anexa a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple con cuatro requisitos copulativos, a saber: a) Estar vinculada al signatario de manera única; b) Permitir la identificación del signatario; c) Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control; Y, d) estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.

En otras palabras, se define la firma electrónica como el conjunto de dígitos o números que aseguran que el creador de la misma es quien efectivamente ha aprobado el contenido del documento firmado.

Respecto a los efectos jurídicos de la firma electrónica la Directiva apuntó a instituir un marco jurídico armonizado para garantizar la eficacia jurídica o que no se negare validez, obligatoriedad y admisibilidad probatoria a una firma distinta de la manuscrita debiendo surtir los mismos efectos jurídicos, presentada en forma de datos electrónicos, pero basada en un certificado reconocido o expedido por un proveedor de servicios de certificación competente.

Respecto a los proveedores de servicios de certificación de firma electrónica Para el caso de redes abiertas, al estimarse innecesario un marco reglamentario dentro de sistemas cerrados, la Directiva solo considera requisitos esenciales mínimos particularmente relacionados con su responsabilidad al expedir los certificados frente a los terceros o consumidores que utilicen sus servicios, de manera tal que existan normas comunes y armonizadas precisamente respecto a dicha responsabilidad y que se permita el reconocimiento de firmas y certificados digitales al interior de toda la Comunidad Europea.

Respecto a la justificación de una acreditación voluntaria, el considerando séptimo explica que el mercado interior permite a los proveedores de servicios de certificación desarrollar actividades transfronterizas para incrementar su competitividad, ante lo cual, para estimular la prestación a nivel comunitario de servicios de certificación en redes abiertas, los proveedores de tales servicios debían gozar en general de libertad para ofrecerlos sin necesidad de autorización previa.

El artículo 6º señala que los Estados miembros deberán velar porque los prestadores de servicios de certificación sean responsables, ante cualquier persona de buena fe que confíe en el certificado, acerca de aspectos tales como la veracidad de la información contenida en el certificado reconocido a partir de la fecha de su expedición, la existencia de dispositivos de creación y verificación de firma, que se puedan establecer límites a los usos del certificado.

3.- LEY ESPAÑOLA DE 1999 Y PROYECTO MODIFICATORIO DE 2001.

El Real Decreto Ley 14/1999, de 17 de septiembre, sobre Firma Electrónica de España en el título primero, disposiciones generales, artículo 2 define firma electrónica como:

> **ARTÍCULO 2.**
>
> **Definiciones:**
>
> "A los efectos de este Real Decreto-ley, se establecen las siguientes definiciones:
>
> a) "Firma electrónica": Es el conjunto de datos, en forma electrónica, ajenos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge (...)."

Observamos que la mencionada ley, en el mismo artículo 2 nos hace una especie de clasificación de la firma electrónica como firma electrónica avanzada conceptual izándola como "la firma electrónica" que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos".

Si analizamos las diferencias existentes entre ambas tenemos que la firma electrónica avanzada además de ser utilizada como medio para identificar al autor del documento que la contiene es creada por medio que el signatario mantiene bajo su control, es decir, que ofrece la ventaja de revelar cualquier cambio realizado en forma posterior.

El Estado español ha tenido una participación activa en el logro de la posición común para proteger la seguridad y la integridad de las comunicaciones telemáticas en las que se emplee la firma electrónica. En ese sentido, existen ya en España diversas normas sobre la presentación de la declaración del Impuesto sobre la Renta de las Personas Físicas por medios telemáticos, dictadas por la Administración tributaria. La Comisión Nacional del Mercado de Valores, por su parte, ha aprobado y puesto en marcha un sistema de cifrado y firma electrónica que se emplea para la recepción de información de las entidades supervisadas. Asimismo, el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social, anuncia la posibilidad de prestar, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, los servicios técnicos y administrativos necesarios para garantizar la seguridad, la validez y la eficacia de la emisión y recepción de comunicaciones, a través de técnicas y medios electrónicos, informáticos y telemáticos. La Fábrica

Nacional de la Moneda y Timbre-Real Casa de la Moneda actuará en colaboración con Correos y Telégrafos.

En el proyecto de Directiva se incorporó, a solicitud del Estado español, una novedad, recogida en el apartado c) del anexo II, entre los requisitos exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos. Esta novedad consiste en permitir que la certificación pueda recoger la fecha y la hora en la que se produce la actuación certificante.

Existe, además, en España un sector empresarial que podría prestar un servicio de certificación de la firma electrónica con suficiente calidad. Se considera que debe introducirse, cuanto antes, la disciplina que permita utilizar, con la adecuada seguridad jurídica, este medio tecnológico que contribuye al desarrollo de lo que se ha venido en denominar, en la Unión Europea, la sociedad de la información. La urgencia de la aprobación de esta norma deriva, también, del deseo de dar, a los usuarios de los nuevos servicios, elementos de confianza en los sistemas, permitiendo su introducción y rápida difusión.

El objeto de este Real Decreto-ley es establecer una regulación clara del uso de ésta, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación. De igual modo, este Real Decreto ley determina el registro en el que habrán de inscribirse los prestadores de servicios de certificación y el régimen de inspección administrativa de su actividad, regula la expedición y la pérdida de eficacia de los certificados y tipifica las infracciones y las sanciones que se prevén para garantizar su cumplimiento.

El Real Decreto Ley 14/1999 nunca tuvo aplicación practica debido a que los prestadores de servicios de certificación nunca se acreditaron, por lo engorroso y complejo de sus requisitos con lo cual el texto pasa a ser letra muerta, por lo que el gobierno español sometió a debate un nuevo texto legal.

B. VALOR PROBATORIO DE LA FIRMA ELECTRÓNICA EN ESPAÑA

El valor probatorio de la firma electrónica en España, esta referido concretamente a la firma electrónica avanzada y para que surta los efectos jurídicos correspondientes es necesario que este basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación

de firma, la cual tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita u ológrafa 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.

Existe la presunción de que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos jurídicos, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado. La eficacia de los certificados sobre dispositivos de seguros de creación de firma, que hayan sido expedidos por los organismos designados para ello, por los Estados miembros de la Unión Europea, será reconocida cuando pongan de manifiesto que dichos dispositivos cumplen los requisitos contenidos en la normativa comunitaria sobre firma electrónica.

Asimismo, tenemos que la firma electrónica que no reúna todos los requisitos no se le negarán efectos jurídicos, ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica.

C. CONSIDERACIONES DE LA LEGISLACIÓN ARGENTINA.

1.- Antecedentes:

En el plano nacional ya existen antecedentes legales y regulatorios, los que se verían mejor sustentados y se beneficiarían del Anteproyecto Ley de Firma Digital al facilitarse la extensión de la aplicación de los sistemas de firma digital ya desarrollados en la Administración Pública Nacional a los Gobiernos Provinciales y Municipales y al sector privado:

a) Decreto Nº 427/98 del Poder Ejecutivo Firmas Digitales para la Administración Pública Nacional. Autoriza el empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa.

La firma digital tiene los mismos efectos de la firma manuscrita, siempre que se hayan cumplido los recaudos establecidos y dentro del ámbito de aplicación en el Sector Público Nacional, dentro del cual se comprende la administración centralizada y la descentralizada, los entes autárquicos, las empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con participación estatal mayoritaria, los bancos y entidades financieras oficiales y todo otro ente, cualquiera sea su denominación o naturaleza

jurídica, en que el Estado Nacional o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones.

La correspondencia entre una clave pública, elemento del par de claves que permite verificar una firma digital, y el agente titular de la misma, se acredita mediante un certificado de clave pública emitido por un certificador de clave pública. Se establecen los requisitos y condiciones para la vigencia y validez de los certificados de clave pública (emisión, aceptación, revocación, expiración y demás contingencias del procedimiento), así como las condiciones bajo las cuales deben operar los certificadores de clave pública licenciados integrantes de la citada Infraestructura de Firma Digital para el Sector Público Nacional. El Decreto fue redactado por el Sub-Comité de Firma Digital del CUPI ("Comité de Usuarios de Procesamiento de Imágenes"), convocado por el Banco Central de la Republica Argentina y del que participaron representantes de distintos organismos estatales.

b) Resolución MTSS n° 555/97 Ministerio de Trabajo y Seguridad Social - Normas y Procedimientos para la Incorporación de Documentos y Firma Digital. Define el documento digital, la firma digital, el certificador de clave pública, el certificado, la clave privada, la clave pública y establece que los

documentos digitales se considerarán válidos y eficaces, surtiendo todos los efectos legales y probatorios cuando estén firmados digitalmente.

c) Resolución SAFJP nº 293/97 Superintendencia de Administradoras de Fondos de Jubilación y Pensiones - Incorporación del Correo Electrónico con Firma Digital. Establece que los CD-ROMS remitidos por las Administradoras de Fondos de Jubilaciones y Pensiones, debidamente identificados por el Sistema, serán válidos y eficaces, surtiendo todos los efectos legales y probatorios, a partir de la fecha y hora en que queden disponibles en las bandejas de entrada y que la firma electrónica o clave de seguridad habilitante para acceder al sistema poseerá el mismo valor legal que la firma manuscrita

d) Resolución SFP nº 45/97 Secretaria de la Función Publica - Incorporación de Tecnología de Firma Digital a los Procesos de Información del Sector Público. La secretaria de la función pública adhiere y hace suyos los conceptos vertidos por el Sub-Comité de Criptografía y Firma Digital del CUPI en el documento "Pautas Técnicas en la Materia de Normativa de Firma Digital" y autoriza el empleo de ésta tecnología para la promoción y difusión del documento y la firma digitales en el ámbito de la Administración Pública Nacional

e) Resolución SFP nº 194/98 Secretaria de la Función Publica - Estándares Aplicables a la Infraestructura de Firma Digital para el Sector Público Nacional del Decreto nº 427/98. La secretaria de la función publica dicta los estándares de homologación de algoritmos criptográficos para la Infraestructura de Clave Pública de la Administración Pública Nacional.

f)Resolución SFP nº 212/97 Secretaria de la Función Publica - Políticas de Certificación para el Licenciamiento de Autoridades Certificantes. La secretaria de la función pública dicta los estándares de licenciamiento y operación de las autoridades certificantes de la Administración Pública Nacional

g) La Resolución general nº 345/99 sobre Documento electrónico y firma digital: En Argentina, la Comisión Nacional de Valores dictó la Resolución general nº 345/99 sobre Documento electrónico y firma digital en el sector privado, en ella reguló los documentos que deben enviarse a través de la AIF, nos encontramos con que se trata de la mayor parte de la documentación societaria que se pone a disposición de los posibles inversores: los estados contables propios y de sus controladas y vinculadas,

los prospectos de emisión, las actas de asamblea, los hechos relevantes y las notificaciones varias.

Todos los documentos o notificaciones que se mencionan se generan, para la Autopista de la Información Financiera (AIF), de forma electrónica, es decir, aparece el documento electrónico; y según Carlos Paladella por el momento, no goza de una regulación positiva en el derecho privado argentino aunque doctrina autorizada empieza a considerar al mismo como si fuera un documento en su concepción más tradicional. En cambio que, para el sector público, se encuentra una mención en la ley 24.624 la cual incorporó un artículo 30 en el que se establecía lo siguiente: "Sustitúyase el artículo 49 de la Ley N° 11.672, Complementaria permanente de presupuesto (t.o. 1995) por el siguiente:

La documentación financiera, la de personal y la de control de la Administración Pública Nacional, como también la administrativa y comercial que se incorpore a sus Archivos, podrán ser archivados y conservados en soporte electrónico u óptico indeleble, cualquiera sea el soporte primario en que estén redactados y construidos, utilizando medios de memorización de datos, cuya tecnología conlleve la modificación irreversible de su estado físico y garantice su estabilidad, perdurabilidad, inmutabilidad e

inalterabilidad, asegurando la fidelidad, uniformidad e integridad de la información que constituye la base de la registración.

Los documentos redactados en primera generación en soporte electrónico u óptico indeleble y los reproducidos en soporte electrónico u óptico indeleble a partir de originales de primera generación en cualquier otro soporte, serán considerados originales y poseerán, como consecuencia de ello, pleno valor probatorio, en los términos del artículo 995 y concordantes del Código Civil.

Este artículo ha sido luego efectivamente reglamentado mediante la Decisión Administrativa 43/1996. Si bien este antecedente puede considerarse la primera piedra para la incorporación a la legislación Argentina del documento electrónico, no cabe duda que la nueva norma de la Comisión Nacional de Valores aporta un elemento indispensable para el uso masivo de este tipo de documento. Ello así, por cuanto, es el sector privado el que está involucrado en el desarrollo de este sistema de intercambio de información y el alcance del mismo permite que se produzcan desarrollos paralelos con similar tecnología. En esta etapa definida por la Comisión permanece la obligación de remitir la información mencionada en la Resolución en el tradicional soporte papel.

Los llamados "documentos electrónicos" han aparecido en el mundo de la informática y no quedan al margen de los problemas jurídicos, comenzando con su definición. De hecho, ha sido en época reciente cuando la ciencia del Derecho se ha encargado de la noción de documento, Carnelutti, citado por Ettore Gianantonio lo define como "una cosa que hace conocer un hecho", coincidiendo con la noción vulgar del término como "cualquier cosa que sirve para ilustrar o comprobar algo

Los documentos electrónicos pueden dividirse en dos categorías: los denominados "documentos electrónicos en sentido estricto" que no pueden ser leídos o conocidos en forma directa por el hombre y que se encuentran memorizados digitalmente contenidos en la memoria central de la computadora o en memorias en masa (*diskettes*, cintas, etc.), y aquellos otros que son confeccionados por el computador por medio de sus periféricos de salida, que son perceptibles, denominados "documentos electrónicos en sentido amplio".

En Congreso Internacional de Informática y Derecho celebrado en Buenos Aires en el año 1990, Alende señala que nada obsta a considerar al documento electrónico dentro de la categoría de "documento", aún cuando no resulta posible categorizarlo como documento público o documento

privado Más precisamente estimamos que se trata del género "prueba documental" a la que debe dársele el mismo tratamiento probatorio; de hecho en el Código General del Proceso de la República Oriental del Uruguay dispone la admisibilidad del documento electrónico como medio de prueba (artículo 146, inciso primero), y lo categoriza como "documento". Esto implica que, en principio, los fax, telefax, correos electrónicos, videogramas, fonogramas, constituyen verdaderos medios de prueba.

La finalidad del Anteproyecto de Ley es eliminar obstáculos al reconocimiento jurídico de las firmas digitales y facilitar la libre circulación de servicios y productos de certificación con otros países. Este Anteproyecto facilita el uso de las firmas digitales en un espacio sin fronteras en lo que concierne a las obligaciones esenciales de las partes intervinientes, y de los certificadores de clave pública.

2. Principios y Objetivos del Anteproyecto Ley de Firma Digital

a) Funcionamiento de las firmas digitales.

El Anteproyecto de Ley apunta a asegurar el buen funcionamiento de las firmas digitales, instituyendo un marco jurídico homogéneo y adecuado para

el uso de estas firmas en el país y definiendo un conjunto de criterios que constituyen los fundamentos de su validez jurídica.

b) No discriminación del documento digital firmado digitalmente.

En un sistema abierto, pero confiable, de firmas digitales, el efecto jurídico atribuido a una firma es un elemento esencial. El presente Anteproyecto de Ley implementa un marco jurídico Nacional que garantiza que la fuerza ejecutoria, el efecto o la validez jurídica de una firma digital no sea cuestionado por el solo motivo de que la firma se presenta bajo la forma de datos digitales, de que ella no se base en un certificado emitido por un certificador de clave pública licenciado, y que las firmas digitales sean reconocidas al nivel jurídico de la misma manera que las firmas manuscritas. Adicionalmente, los regímenes nacionales de admisibilidad de pruebas se extienden para incluir la utilización de firmas digitales.

c) Libertad contractual.

La tecnología de firmas digitales tiene aplicaciones evidentes en entornos cerrados, como ser la red local de una empresa o un sistema bancario. Los certificados de clave pública y las firmas digitales tienen igualmente una función de autorización, por ejemplo para acceder a una cuenta personal. En el marco de la legislación nacional, el principio de la libertad contractual

permite a las partes contrayentes convenir entre ellas la modalidad de sus transacciones, es decir, si ellas aceptan o no las firmas digitales. En este caso, no se manifiesta una necesidad evidente de legislación.

d) No obligación de obtener licencia, licenciamiento no obligatorio

Teniendo en cuenta la gama de servicios en cuestión y sus posibles aplicaciones, los certificadores de clave pública prestatarios de servicios de certificación pueden ofrecer sus servicios sin la obligación de obtener una licencia. De todos modos, estos prestatarios de servicios pueden optar por beneficiarse de la validez jurídica que le confiere a las firmas digitales el régimen voluntario de licenciamiento de ésta ley. El licenciamiento debe considerarse como un servicio público ofrecido a los prestatarios de servicios de certificación que deseen ofrecer un servicio de alto nivel. Esto no debe en ningún caso implicar que un prestatario no licenciado sea automáticamente menos seguro.

e) Otros servicios de certificación relacionados a las firmas digitales.

Un certificador de clave pública prestatario de servicios de certificación puede ofrecer una amplia gama de servicios. El presente Anteproyecto de Ley se centra particularmente en los servicios de certificación relacionados con las firmas digitales. Los certificados pueden utilizarse con fines muy diversos y

contener diferentes datos. Puede tratarse de identificadores clásicos, como ser el nombre, la dirección, el número de documento de identidad, el número de contribuyente o de identificación fiscal o cualquier atributo específico del firmante, por ejemplo, que permiten establecer si está facultado para actuar en nombre de una empresa, si es solvente, si tiene garantes o si es titular de permisos o de licencias particulares.

Como consecuencia, se puede visualizar la emisión de diversos tipos de certificados para múltiples usos. Sin embargo, un marco jurídico es necesario sobre todo para los certificados, a fin de permitir el autenticado de la firma digital del firmante. Por ello, el Anteproyecto tiene como objeto regir el funcionamiento de los certificadores de clave pública, licenciados y no licenciados, que emiten certificados de clave pública en relación con la identidad civil de una de las personas determinadas de existencia visible.

f) Criterio de proporcionalidad.

El reconocimiento jurídico de firmas digitales debe reposar sobre criterios objetivos, transparentes, no discriminatorios y proporcionales, que no deben ser condicionados a ninguna autorización o licenciamiento del prestatario del servicio respectivo. Las exigencias comunes aplicables a los prestatarios de servicios de certificación deben permitir el reconocimiento internacional de

firmas y certificados para los países del Mercosur y del mundo que cuentan con un marco normativo compatible.

g) Responsabilidad.

En materia de responsabilidad, las reglas comunes deben contribuir a suscitar la confianza de los usuarios y de los suscriptores y de las organizaciones, que confíen en los certificados y en los prestatarios de servicios y promover así una amplia difusión de las firmas digitales.

Respecto de los certificadores se excluye la responsabilidad de los certificadores de clave pública, éstos no deberán ser responsabilizados por las eventuales inexactitudes en los certificados emitidos que resulten de la información facilitada por el solicitante, siempre que el certificador pueda demostrar que ha tomado todas las diligencias necesarias según que exigiere la naturaleza de la obligación, y que correspondiesen a las circunstancias y el tipo de certificado de que se trate de las personas, del tiempo y del lugar para verificar tal información.

Los certificadores de clave pública deberán poder podrán consignar en los certificados que emitan los límites establecidos para su utilización, tal que el certificador no sea responsable por los daños y perjuicios que resulten del

uso no autorizado de un certificado en el que consten dichos límites de utilización. Los certificadores de clave pública también deberán poder consignar en los certificados que emitan un valor límite de las transacciones válidas que puedan realizarse mediante el mismo, tal que el certificador no sea responsable de los eventuales daños y perjuicios que excedan de dicho valor límite.

h) Operación internacional reconocimiento de certificados emitidos en otros países.

Los mecanismos cooperativos y un marco normativo compatible que permitan el reconocimiento entre países de las firmas y de los certificados, son esenciales para el desarrollo del comercio electrónico internacional. En particular, permitir a los prestatarios de servicios de certificación dentro del ámbito del MERCOSUR, avalar garantizar los certificados de terceros países de la misma forma que garantizan a sus los propios certificados, constituye un medio simple pero eficaz de promover los servicios internacionales y la integración.

D. VALOR PROBATORIO DE LA FIRMA ELECTRONICA EN CHILE

En un proceso civil inspirado por el principio dispositivo el juez asume un rol activo al valorar la prueba rendida por las partes, con el objeto de lograr el establecimiento material de los hechos, dándolos por probados o no luego de su análisis. Es decir, al valorar la prueba se busca determinar la eficacia de los diversos medios probatorios y la influencia que ejercen sobre la resolución.

Sin embargo, existen diversos sistemas de valoración, destacando aquellos de las pruebas legales y los de las pruebas libres o de libre convicción. En un sistema de prueba legal la ley le señala al tribunal, a priori, el grado de eficacia justificativa de determinados elementos probatorios que ella misma establece; son pruebas estrictas, por cuanto privan al tribunal de cualquiera intervención personal o subjetiva en la apreciación, y al efectuar ésta, debe sujetarse a normas preestablecidas por la propia ley. Por su parte, en un sistema de libre convicción se permite mayor discrecionalidad al juez, quien puede fallar incluso en contra de las pruebas rendidas y decidir en conciencia.

Entre ambos sistemas, surge el de la sana crítica que, al combinarlos y morigerarlos, conduce a un fallo justo y equitativo. Según este sistema, el tribunal debe asesorarse por sus conocimientos técnicos, su experiencia personal, la lógica, el sentido común, el buen juicio y la recta intención.

Lo anterior significa que en un ordenamiento jurídico que recoja el sistema de prueba legal, es necesario que la ley considere expresamente al documento electrónico como medio de prueba idóneo. En cambio, según el principio del libre convencimiento del juez, las partes podrán acompañar documentos electrónicos y el juez no tendrá obstáculos para admitirlos como medios de prueba, en la medida en que no exista norma alguna que lo inhiba para utilizar los documentos electrónicos como medios de prueba, admitiéndolos en subsidio de otros, imponiéndoles una determinada eficacia probatoria.

Pero esto no significa que el juez debe necesariamente atribuirle plena atendibilidad al documento electrónico, sin valorar antes su autenticidad y su seguridad. Así, el documento será auténtico cuando no haya sufrido alteraciones, cuando ha sido realmente otorgado y autorizado por la persona y de la manera que en él se expresa, y será tanto más seguro cuanto más difícil sea alterarlo y cuanto más fácil sea verificar la alteración y reconstruir el texto originario.

En Chile, las leyes reguladoras de la prueba han establecido un sistema legal de prueba tasada, es decir, es la ley la que establece los medios de prueba, la forma de rendirla en juicio y, en ciertos casos, la valoración que debe darle el juez, o sea las pruebas pueden llegar a tener un valor inalterable y constante, señalado en la ley, que fija condiciones generales de hecho abstractamente preestablecidas que se aplican en todas las hipótesis que presentan aquellos caracteres, y se prescinde del criterio o apreciación del juez respecto de los mismos hechos.

Las normas generales de tal sistema se recogen en el Código Civil, que se preocupa de reglamentar la admisibilidad de los medios de prueba y su valor probatorio, y además, en el Título XI del Libro II del Código de Procedimiento Civil, donde enumera los medios de prueba, reglamenta la manera de cómo se produce la prueba ante los tribunales, y en algunos casos su valor probatorio. Ello, sin perjuicio de lo establecido en el Código de Procedimiento Penal cuando la materia sea criminal.

Sin embargo, en cuanto a la valoración de la prueba rendida, este sistema se aplica en forma limitada, resultando ser la excepción, admitida sólo cuando la ley la establece de modo expreso, como en el caso de la plena fe que

atribuye al instrumento público, al instrumento privado reconocido, a la confesión judicial sobre un hecho personal y la limitación a la prueba de testigos. No obstante, estas reglas desaparecen en aquellos casos en que el juez está facultado para apreciarla en conciencia.

Es decir, la regla general aplicable en la legislación chilena para la apreciación de las pruebas rendidas es el sistema de la libre convicción, en donde el juez debe atenerse a los medios de prueba que señala la ley, pero valora esos elementos conforme a la convicción que se forme de los hechos, debiendo fundamentar la sentencia dando razón de la labor de crítica que le mueve a pensar en cierta forma.

Hay ciertos casos en que la ley chilena expresamente señala que la prueba se apreciará en conciencia, lo que no difiere del sistema en estudio, constituyendo una contra excepción a los casos en que el valor lo establece la ley. Ello ocurre, por ejemplo, en los juicios laborales regidos por el Título I del Libro IV del Código del Trabajo; en los juicios seguidos ante un Juez de Letras de Menores; o en los de arrendamiento de bienes raíces urbanos, entre otros, pero esto no significa que la apreciación de la prueba quede entregada al libre arbitrio del juez, sin tener que formarse una entera convicción fundamentada.

En conclusión, en materia de valoración el sistema de persuasión racional o de la libre convicción es la regla general, con algunas manifestaciones de prueba legal, las que el legislador atenúa en muchos casos mediante la apreciación en conciencia.

Sin perjuicio de lo anterior, la determinación de los medios idóneos para acreditar un hecho en juicio y la forma en que esta prueba debe ser rendida, le corresponde señalarlo a la ley exclusivamente, ya que el sistema chileno no es de prueba libre sino que legal.

De lo anterior se podría pensar que la rigidez propia de un sistema legal de prueba, no admitiría estas nuevas tecnologías, pero la negación a aceptar a los documentos electrónicos como medios de prueba no se justifica suficientemente debido a la indefensión o la impunidad que acarrearía a quienes se desenvuelven en una sociedad tecnológica que contradictoriamente no le proporciona medios para acreditar sus pretensiones.

Es decir, en el sistema procesal reglado chileno, la admisibilidad de una prueba dependerá de aplicar un medio regulado en la ley. Esto nos lleva a

distinguir entre aquellas situaciones en que el documento electrónico está expresamente considerado como medio de prueba y aquellas en que hay un vacío legal.

En Chile, el artículo 341 Código de Procedimiento Civil fija como los medios de prueba de que puede hacerse uso en juicio a los instrumentos, los testigos, la confesión de parte, la inspección personal del tribunal, el informe de peritos y las presunciones. Además, el ordenamiento jurídico civil en ninguna disposición ha incorporado expresamente y de un modo general a los documentos electrónicos dentro de los medios de prueba. Por lo tanto, ante esta situación hay que ver la forma de presentarlos en juicio.

No hay duda que en los casos en que la ley alude a ellos expresamente dándole el carácter de instrumento público o privado los tribunales deben reconocerles mérito probatorio. Así por ejemplo, en el artículo 913 del Código de Comercio señala que las anotaciones en el diario de navegación (un instrumento público) pueden estamparse por medios mecánicos o electrónicos que garanticen la fidelidad y permanencia de los datos. Más adelante, en el artículo 1014 señala que la firma en el conocimiento de embarque puede ser registrada por cualquier medio mecánico o electrónico. Por su parte, la Ley 19.052, de 14 de abril de 1991 consagró explícitamente

el carácter de instrumento público de los certificados que el Servicio de Registro Civil e Identificación expide mecanizadamente, a través del procesamiento electrónico de datos, sin intervención del hombre y sin firma manuscrita. Ello, entre otros cuerpos legales.

Pero, sin duda, el problema se presenta cuando la ley nada dice respecto a la admisión y valor de los documentos electrónicos. Por tanto, veamos si es suficiente la legislación procesal civil y penal chilena actual para abordar la prueba mediante un documento electrónico.

El primer punto a considerar es asimilar el documento electrónico con algún medio de prueba legal. Ya lo sostenía de tal manera el profesor uruguayo Eduardo Couture al escribir:

> "Cuando se trata de fijar el régimen procesal de los diversos medios de prueba no especialmente previstos, se hace necesario asimilarlos a los especialmente previstos. Así, la impresión dactiloscópica, la fotografía y radiografía, se rige por los principios de la prueba documental; es asimismo, un documento en sentido amplio, el disco sensible en que se ha grabado una voz, un ruido o un período musical, la prueba hematológica, la autopsia y la misma radiografía caen directo del campo de la prueba pericial".

Frente a este tema nos interesa específicamente referirnos a la prueba documental, debido a que el fenómeno probatorio, principalmente respecto a la prueba instrumental, ha encontrado en las tecnologías de la información

importantes cambios. Aunque en nuestra legislación se emplean confusa e indistintamente las voces documento e instrumento, somos de la idea de considerar al primero como el género, más amplio porque abarca cualquier medio de expresión del pensamiento, y limitar el segundo a los documentos que se concretan en la escritura.

Ello nos lleva a responder si los documentos electrónicos pueden o no ser considerados documentos escritos, y luego, si se encuadran en la clasificación entre instrumentos públicos o privados.

La comunicación escrita requiere la fijación de un mensaje sobre un soporte material y a través de un lenguaje. Como el documento electrónico contiene un mensaje (desde un texto alfanumérico hasta un diseño o un gráfico), escrito en un lenguaje de dígitos binarios (*bits*), sobre el soporte material mueble que le brindan los dispositivos de memoria secundaria (por ejemplo, los discos magnéticos), y además, supera las limitaciones temporales y espaciales de la comunicación oral al no necesitar que emisor y receptor se encuentren físicamente presentes el uno del otro, no hay duda que nos permite concluir afirmativamente sobre el valor de acto escrito del documento electrónico.

No creemos suficientemente sólida la crítica que reciben los documentos electrónicos en sentido estricto, a los cuales se les pretende negar el carácter de acto escrito por no ser perceptibles y comprensibles directamente por el hombre, ya que no hay duda que un mensaje redactado en un lenguaje convencional pero secreto puede ser considerado escrito.

Sin embargo, existen dudas más importantes con relación al carácter de instrumento público o privado que pueda tener un documento electrónico.

El artículo 1699 del Código Civil define al instrumento público o auténtico como el autorizado con las solemnidades legales por el competente funcionario. Esto implica que para que el documento electrónico sea considerado como tal requiere los siguientes requisitos:

1. Ser autorizado por un funcionario público competente. Dicho funcionario debe haber sido investido en su cargo previamente en forma legal, y estar actuando dentro del ámbito de sus atribuciones, tanto en la materia como en el territorio. Por ejemplo, un Oficial del Registro Civil que emite electrónicamente un certificado de nacimiento.

2. Debe otorgarse con las formalidades que la ley señala, las cuales variarán en cada caso.

Ahora bien, complementariamente, el artículo 342 del Código de Procedimiento Civil señala que se considerarán como instrumentos públicos en juicio a los documentos originales. Este punto nos remite a lo dicho sobre la originalidad del documento electrónico y a la necesidad de que el legislador aclare esta situación.

Finalmente, también serán instrumentos públicos en juicio ciertas copias de los documentos originales, a saber, las copias autorizadas conforme a las formalidades que las leyes exigen sobre este particular; las copias simples (que no cumplen los requisitos anteriores) pero que no se objetan como inexactas dentro del plazo legal; las copias simples objetadas como inexactas por la parte contraria, pero que se comparan o cotejan con el original y se hallan conforme a éste; y finalmente, las copias que el tribunal mande agregar durante el juicio, incluso las incompletas aunque no inexactas.

En conclusión, es perfectamente posible que un documento electrónico pueda ser considerado como un instrumento público si se adecua a las reglas generales.

En cambio, creemos que la naturaleza de los documentos electrónicos en sentido estricto riñe con la del instrumento privado. En un sentido amplio, el instrumento privado es todo escrito que da constancia de un hecho y que ha sido otorgado por los particulares sin intervención de funcionario público competente u otros requisitos o formalidades, salvo por la firma.

Creemos que un requisito esencial de la escritura privada es la firma, esto es, la imposición del nombre propio y el apellido por parte de la persona de la cual resultan provenir las declaraciones y que representa la conformidad de la voluntad con aquello que aparece escrito precedentemente. Sin embargo, hacemos presente que existe un divorcio en la doctrina sobre este punto.

Para algunos autores, los instrumentos privados pueden o no estar firmados por las partes; y pueden, incluso, hasta omitir la fecha y el lugar en que han sido otorgados, porque en el derecho positivo no se exige ningún requisito o solemnidad para conformarlos. Esta posición doctrinal no encontraría ningún inconveniente para admitir como instrumento privado a un documento

electrónico en sentido amplio o estricto, sin perjuicio de tener que ceñirse a las reglas generales para su admisión en juicio, esto es, ser reconocido por la parte a quien se opone o ser mandado tener por reconocido en los casos prevenidos por ley.

Nosotros pensamos que el instrumento privado debe estar firmado por los otorgantes, porque la firma es el signo que demuestra que se aprueba y hace propio lo escrito. Sin la firma, el documento no pasa de ser un borrador. Nos apoyamos en el propio Código Civil, por ejemplo en el artículo 1701 inciso 2°, que sostiene que el instrumento público defectuoso por incompetencia del funcionario o por otra falta en la forma, valdrá como instrumento privado si estuviere firmado por las partes; en el artículo 1702, que le reconoce valor de escritura pública al instrumento privado, respecto de los que aparecen o se reputan haberlo suscrito; el artículo 1703, que dice que la fecha de un instrumento privado no se cuenta respecto de terceros sino, entre otros casos, desde el fallecimiento de alguno de los que lo han firmado.

También la Corte Suprema ha considerado esencial la firma por estar en ella la garantía de autenticidad, debido a que significa la aprobación o aceptación de lo que en ellos está consignado. Sin embargo, no ha sido suficientemente clara la respuesta de la jurisprudencia ya que en una sentencia posterior

señaló que no es necesaria la firma en esta clase de documentos, pues no tiene más significación que la meramente formal de un elemento testificativo, que se requiere no para la validez del documento sino para que haga fe en relación con las declaraciones que emiten en él las partes que se obligan.

Por lo tanto, creemos que un documento electrónico en sentido estricto no puede ser considerado un instrumento privado mientras no se homologue la firma electrónica con la firma manuscrita. Ello se justifica, entre otros argumentos, porque la función que presenta el acto de la suscripción se puede obtener tanto en una firma electrónica como en una manuscrita. En ambas se apreciaría una función indicativa, ya que sirven para señalar al autor del documento; una función declarativa de asunción de la paternidad del documento; y una función probatoria que permite verificar si el autor de la firma es efectivamente aquel que ha sido indicado en la suscripción misma.

Lamentablemente, el desconocimiento sobre las firmas electrónicas y el apego absoluto a la no siempre precisa presunción de que cada individuo tiene un modo particular de firmar nunca perfectamente reproducible, ha llevado a requerir únicamente la rúbrica autógrafa, o sea, impuesta de puño y letra por parte del firmante, aunque sea extendida con letra de imprenta, pero no con medios mecánicos. De allí, debemos reconocer al documento

electrónico en sentido estricto valor de documento escrito, eventualmente de instrumento público, pero no de instrumento privado por la imposibilidad del acto de suscripción personal.

En otro sentido, y como señalamos anteriormente, la idea de admitir analógicamente documentos no contemplados dentro de los medios de prueba, ha sido avalada por nuestros Tribunales. Por ello, en los casos en que se presentaban esos documentos, por ejemplo, una fotografía, se les regulaba como instrumentos, y así, en el proceso civil se les aplicaban las disposiciones de los artículos 342 a 355 del Código de Procedimiento Civil, y en el proceso penal, los artículos 184 a 188 del Código de Procedimiento Penal. Todo esto producía dificultades especialmente cuando se objetaban los documentos. Imperaban, entonces, las pruebas periciales y de presunciones.

Sin embargo, con la Ley N°18.857, que reformó el Código de Procedimiento Penal en 1989, se mejoró esta situación en el proceso penal, especialmente en lo que se refiere a los documentos, admitiendo como elementos de prueba "las 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" (artículo 113 *bis*).

A su vez, realizada la reforma al artículo 113, la misma permite al juez, para el esclarecimiento de los hechos, disponer de "la fotografía, filmación o grabación y, en general, la reproducción de imágenes, voces o sonidos por los medios técnicos que estime convenientes. Asimismo, podrá valerse de resultados obtenidos por la utilización de aparatos destinados a desarrollar exámenes o demostraciones científicas o por medio de la computación".

Es decir, la ley procesal penal, en su artículo 113 *bis*, no asimila estos nuevos elementos de prueba a los instrumentos, sino que los considera como documentos y los estima como base de presunciones o indicios, según exista o no una relación precisa y directa entre el hecho acreditado y el que se trata de probar.

En caso que haya objeciones o impugnaciones a las reproducciones acompañadas al proceso, entra en juego la prueba pericial o de técnicos, algunas de las cuales se han reglamentado especialmente por su importancia, como las de los marcadores genéticos sanguíneos en la investigación biológica de la paternidad o la fotografía dactiloscópica como medio de autenticación documental infalible.

En síntesis, la jurisprudencia ha aceptado desde antes de la reforma de la Ley N°18.857 el concepto amplio de prueba documental para comprender las modalidades de prueba que se mencionan en los artículos 113 y 113 bis del Código de Procedimiento Penal. Con las modificaciones de la ley mencionada no hay problemas en el proceso penal para admitir como elementos de prueba a los documentos electrónicos.

Sin embargo, la cuestión subsiste en el proceso civil donde hay que auxiliarse más que del concepto amplio de documento, en la prueba pericial y de presunciones. Veamos, la revolución en las comunicaciones que ha generado la telemática explica el empleo cada vez más común del correo electrónico por ejemplo, un medio más rápido e interactivo que una carta tradicional, aunque opera de manera similar. Para analizar el valor probatorio que puede tener este tipo de correo, tenemos que asimilarlo al de las cartas y los telegramas. No obstante, el Código Civil chileno no señala expresamente el valor probatorio de éstos, pero entendemos que el destinatario de una carta puede invocarla como prueba contra el que la ha escrito; puede utilizarla para establecer una obligación contraída a su favor por el remitente; para probar un perjuicio que éste le ha causado o una injuria en su contra que dé motivo a una demanda de indemnización. Además, si la carta no es confidencial, el destinatario puede hacerla valer en juicio contra

una persona distinta del remitente; pero si la carta tiene el carácter de confidencial o íntimo, no puede utilizarse contra un tercero sino con autorización del que la envió.

El artículo 349 del Código de Procedimiento Civil es atinente a esta materia al referirse a los documentos que existan en poder de la otra parte o de un tercero y tengan relación directa con la cuestión debatida; puede decretarse su exhibición a petición de parte, siempre que no revistan el carácter de secretos o confidenciales.

Si las cartas están firmadas pueden constituir verdaderos instrumentos privados, por el contrario si no lo estuvieran o sí en ellas no hay explícitamente una declaración de voluntad, pueden tener el mérito de una confesión extrajudicial escrita o de un principio de prueba por escrito, conforme al valor que el juez les atribuya, si están reconocidas.

En definitiva, como la ley chilena no ha reglamentado el valor probatorio de estos documentos, queda entregada a la apreciación del tribunal. Por eso, no puede entenderse que estas comunicaciones privadas carecen de todo valor probatorio.

Si el documento es objetado, los interesados pedirán lo que corresponda para ofrecer la prueba necesaria. Pero, si no se desconoce el hecho de que emana realmente de la persona que lo firma, y aún no se impugnan los datos allí indicados, no se ve la conveniencia de negarle todo valor; puede el juez apreciarlo libremente, conforme a la persuasión racional.

Incluso si carece de firma o ésta no es reconocida por la ley, como el caso de la firma electrónica, la por sello o la calcada, esto sólo significa que en estos casos la firma no basta por sí sola para dar pleno valor al instrumento público o privado. El valor de este documento lo determinará el juez, ya que servirá de base para una presunción judicial. Piénsese en los documentos normalizados, que están pre-redactados y que sólo hay que rellenar los espacios en blanco, generalmente con un signo convencional, para manifestar la voluntad o intención de una persona. Aunque no está firmado puede servir de base para un reconocimiento, por aplicación, en la vía civil, del artículo 346 del Código de Procedimiento Civil.

Otro caso es el de los documentos electrónicos en sentido amplio, que podemos asemejar al de las fotocopias. En el Código de Procedimiento Civil se habla de copias al referirse el artículo 342 a los instrumentos públicos. Naturalmente, en la época de su dictación (1893) no se aludió a las

fotocopias, ya que eran desconocidas. Con posterioridad, el Decreto Ley 407, de 19 de marzo de 1925, creó una norma que después fue incorporada al artículo 422 del Código Orgánico de Tribunales: "las copias (de escrituras públicas) podrán ser manuscritas, dactilografiadas, impresas, litografiadas, fotografiadas o fotograbadas; en ellas deberá expresarse si son primeras o segundas copias, y se estampará el signo o sello del notario autorizante".

Esta disposición autoriza el uso de la fotocopia en los instrumentos notariales. Los jueces las aceptan, y a diario se ve como se otorgan fotocopias de sentencias u otras actuaciones. Si éstas son objetadas, entonces deben ser cotejadas con su original o con otras copias que hagan fe respecto de la parte contraria, a fin de que el tribunal resuelva si se hallan conformes.

En relación con el valor como instrumento privado, la jurisprudencia y la doctrina han señalado que la fotocopia no valdría como tal porque en ellos falta la firma. Sin embargo, si existe el original y es posible hacer el cotejo en caso de impugnación, no se ve el inconveniente para aceptarlas, igualmente si la fotocopia lleva la autorización de un notario que certifique haber tenido a la vista el original y que las partes otorgantes reconocieron su firma ante él.

Finalmente, hoy las técnicas de multimedios permiten integrar imagen, video, texto y sonido en algunos documentos. Los tribunales franceses han concluido que las grabaciones sonoras pueden ser consideradas documentos sin que haya un texto expreso que así lo diga. Ahora, en cuanto a su valor probatorio, no pueden asimilarse al valor del instrumento privado, ya que un requisito esencial de éste, es que esté firmado, pero sí puede dársele el valor de un principio de prueba por escrito o de una confesión. Es importante en este punto tener en consideración que el valor probatorio de las grabaciones sonoras tiene un límite, que es el derecho de las personas a que se respete el secreto de sus conversaciones privadas.

Acerca de lo dicho, hay un fallo muy importante de la Corte de Apelaciones de Santiago, que declara que "una grabación original, efectuada en *casete*, que no se encuentra contemplada en nuestra legislación en forma específica como medio de prueba, puede ser asimilada a la instrumental por registrar hechos o a las confesiones extrajudiciales, de conformidad con lo dispuesto en el artículo 398 del Código de Procedimiento Civil y atribuirle valor en conciencia, acreditado, mediante peritaje, que las voces registradas en la grabación corresponden a las partes del juicio, que la trascripción que rola en autos corresponde a lo grabado y que su tenor guarda armonía con las

demás probanzas del proceso, lo que hace presumir su veracidad, particularmente como confesión extrajudicial del demandado.

No obsta a la conclusión anterior que la grabación haya sido efectuada sin conocimiento del demandado y que éste haya negado haber sostenido la conversación de que se trata con el demandante y que una de las voces le pertenezca, ya que tales negativas aparecen desmentidas por el informe pericial inobjetado".

Esta sería la primera sentencia que se dicta en materia no penal, dando por acreditados los hechos a través de un medio de prueba distinto de los tradicionales, en este caso, de una grabación magnetofónica.

Por su parte, la doctrina chilena ya se ha pronunciado sobre el valor de estos nuevos medios de prueba. Por ejemplo, Enrique Paillás en su obra "Estudios de derecho probatorio", estima que a la grabación no puede dársele el mérito de un instrumento privado en sentido propio, pero sí puede dársele el valor de un principio de prueba por escrito o de una confesión judicial.

El profesor Carlos Ducci en su obra "Derecho Civil, Parte General", y al tratar los nuevos medios de prueba, contempla la posibilidad de asimilar las

grabaciones a los instrumentos privados y señala que, en todo caso, pueden tener valor como elemento probatorio sirviendo de base a una presunción judicial.

Finalmente, don Juan Agustín Figueroa en sus trabajos que aparecen en "Nuevas orientaciones de la prueba", analiza la grabación mecánica de la voz como eventual medio probatorio, sosteniendo que la propia voz puede ser considerada como una "firma" en la grabación magnetofónica pues contiene los tres elementos de la esencia de la firma: la intencionalidad, la personalidad y la inmutabilidad.

La presente sentencia estima la grabación, cuya autenticidad se ha probado, como una confesión extrajudicial. De acuerdo con el artículo 398 del Código de Procedimiento Civil, "la confesión extrajudicial es sólo base de una presunción judicial, y no se tomará en cuenta, si es puramente verbal, sino en los casos en que sería admisible la prueba de testigos".

Es decir, existe reconocimiento jurisprudencial que avala nuestra postura y que permitiría admitir y valorar, si aplicamos la analogía, un documento electrónico en sentido estricto.

E. LEY DE FIRMA DIGITAL EN ALEMANIA (BUNDESGESETZBLATT 1977 TEIL I SEITE 1872-6).

El propósito legislativo y el ámbito de aplicación de esta Ley, se encuentra contemplado en su artículo al señalar:

> "El propósito de este Decreto es establecer condiciones generales bajo las cuales las firmas digitales serán consideradas seguras y las falsificaciones o manipulaciones de firmas digitales o información firmada puedan ser detectadas con alto grado de fiabilidad.
> La aplicación de otros procedimientos de firma digital es opcional en aquellos casos en que la firma digital no sea requerida de acuerdo con este Decreto por las estipulaciones legales".

a. Definiciones:

> "(1) Una firma digital en el sentido de esta Ley es un sello añadido a los datos digitales generado mediante una clave privada de firma y establece el propietario de la firma y la integridad de los datos con la ayuda de una clave pública asociada suministrada mediante un certificado de clave de firma por un organismo certificador o la autoridad de acuerdo con el Nº 3.
>
> (2).Una entidad certificadora en el sentido de esta Ley es una persona física o jurídica que certifique la asignación de claves públicas de firma a personas físicas para lo cual dispone de una licencia de acuerdo al Nº 8
>
> (3) Un certificado en el sentido de esta Ley es un significado digital (autentificado mediante una firma digital) de la asignación de una clave pública de firma pública a una persona física (certificado de clave de firma) u otros certificados digitales que contengan otra

información y que se refieran claramente a un certificado de clave de firma específico (certificado de atributos).

(4) Un sello de tiempo en el sentido de esta Ley es una declaración digital (autentificada mediante una firma digital) emitida por una autoridad certificadora, confirmando que una información digital específica le fue presentada en un momento concreto."

b. Autoridad competente.

"La concesión de licencias, la expedición de certificados utilizados para la firma de certificados, y la supervisión de acuerdo con esta Ley y con la Ordenanza que tiene fuerza Ley conforme al Nº 16 que incumben a la autoridad de acuerdo con Nº 66 de la Ley de Telecomunicaciones".

c. Licencia a las Entidades Certificadoras.

"La actividad de una entidad certificadora requerirá una licencia de la autoridad competente. Una licencia se concederá a raíz de una solicitud.

(1) Una licencia podrá ser denegada cuando los hechos justifiquen la suposición de que el solicitante no posee la fiabilidad necesaria para actuar como entidad de certificación, cuando el solicitante no aduce prueba del conocimiento especializado que requiere la utilización de una autoridad de certificación o cuando haya razón para creer que, que al empezar a utilizarla, los otros requisitos pertenecientes a la utilización de la entidad de certificación expuestos en esta Ley y en el Decreto de acuerdo con el Nº 16 no se cumplan.

(2) Cualquiera que como operador de una entidad de certificación, garantice el cumplimiento con las estipulaciones legales aplicables al funcionamiento de tal entidad, será considerado poseedor de la fiabilidad necesaria. El conocimiento especializado requerido será considerado válido cuando las personas comprometidas en el funcionamiento de la autoridad de certificación tengan el

conocimiento necesario, experiencia y habilidades. Los demás requisitos referentes a la operación de la entidad de certificación se considerarán cumplidos cuando la autoridad competente haya notificado por medio de plazo por medio de un concepto de seguridad de las medidas aseguradoras de acuerdo con los requisitos de seguridad de esta Ley y el Decreto de acuerdo con Nº 16, y su realización haya sido comprobada y confirmada por una persona reconocida por la autoridad competente.

(3) Se pueden adjuntar cláusulas colaterales a una licencia, cuando sea necesario para asegurar el cumplimiento por la entidad de certificación, con los requisitos de esta Ley y el Decreto de acuerdo con el Nº 16.

(4) ..La autoridad competente expedirá los certificados para las claves de firma autorizados para añadir firmas a certificados. Las estipulaciones aplicables a la expedición de certificados por autoridades de certificación se aplicarán de acuerdo con la autoridad competente. La autoridad competente guardará los certificados que haya expedido y los hará accesible en cualquier momento, y a cualquier persona, a través de enlaces de telecomunicación públicos. Esto también se aplicará a la información referente a las direcciones y números de acceso de las entidades de certificación, invalidez de certificados emitidos por la autoridad competente, cese y prohibición de la operación de una autoridad de certificación así como la retirada o revocación de licencias.

(5) ..Cualquier servicio público entregado de acuerdo con este Decreto y la ordenanza que tiene fuerza de ley de acuerdo con & 16 estará sujeto a costes (honorarios y gastos)."

d. Expedición de certificados

(1) .La entidad de certificación establecerá fidedignamente la identidad de personas que soliciten un certificado. Esto confirmará la asignación de una clave pública de firma a una persona identificada por un certificado de clave de firma el cual, junto en cualquier

certificado atributivo, será guardado válido para verificación y, con el consentimiento del propietario de la clave de firma, para la recuperación en cualquier momento y por cualquier persona mediante enlaces de telecomunicación válidos.

(2) .A petición de un solicitante la entidad de certificación incluirá el certificado de clave de firma o información certificada relacionada con su autoridad para representar a una tercera parte y a su admisión profesional a ejercer, o cualquier otra clase de admisión como una prueba fidedigna provista del consentimiento por la tercera parte a la inclusión de la autoridad de representación o de la admisión.

(3) .A petición de un solicitante la entidad de certificación indicará un seudónimo en el certificado, en vez del nombre del solicitante.

(4) .La entidad de certificación tomará medidas, para prevenir cualquier falsificación no detectada o manipulación de los datos de los certificados. También se tomarán medidas para asegurar la confidencialidad de las claves privadas de firma de firma. No se permitirá el almacenamiento de claves privadas de firma por una entidad de certificación.

(5) ..La entidad de certificación contratará a personal de confianza para el ejercicio de actividades de certificación. Para la estipulación de claves de firma y la expedición de certificados utilizarán componentes técnicos como los expuestos en & 14. También aplicarán a los componentes técnicos, la capacidad para la verificación de cerificados de acuerdo con el párrafo 1, frase 2."

e. Requerimiento de notificación

"La entidad de certificación notificación a los solicitantes de acuerdo con Nº 5 (1) las medidas necesarias para mantener las firmas digitales seguras y su verificación fiable. Notificará a los solicitantes de los componentes técnicos que cumplen los requisitos de Nº 14 (1) y (2), y la asignación de firmas digitales generadas por una clave privada de firma. Aconsejará A los solicitantes que los datos, que lleven una firma digital pueden necesitar ser firmados otra vez, antes de que la seguridad de la firma existente disminuya con el tiempo."

f. Contenido de los certificados

"El certificado de clave de firma debe contener la siguiente información:

1. El nombre del propietario de la clave de firma, cuya información adicional se debe adjuntar en caso de posible confusión, o un seudónimo distintivo asignado al propietario de la clave de firma, claramente señalado como tal.
2. Clave de firma pública asignada.
3. Nombre de los algoritmos, con los que la clave pública del propietario de la clave de firma así como la clave pública de la entidad de certificación se puedan utilizar.
4. Número del certificado.
5. Principio y fin del período de validez del certificado.
6. Nombre de la entidad de certificación y
7. Una indicación, de si el uso de la clave de firma está restringido en tipo o ámbito en solicitudes especificas.

8. La información relacionada con la facultad para representar a una tercera persona y la admisión profesional para ejercer u otro tipo de admisión puede ser incluido tanto en el certificado de clave de firma como en un certificado de atributos.
9. La autoridad competente invalidará los certificados que ha expedido de acuerdo con el N° 4 (5) cuando una entidad de certificación cese en su funcionamiento o su licencia sea retirada o revocada."

g. Sello de tiempo.

"Bajo petición, la entidad de certificación pondrá el sello de la fecha de expedición a datos digitales."

h. Documentación.

"La entidad de certificación documentará las medidas de seguridad para el cumplimiento de esta Ley y el Decreto de acuerdo con Nº 16 y los certificados expedidos, de modo que los datos y su integridad pueden ser verificados en cualquier momento."

i.- Cese del funcionamiento.

(1) "En el cese del funcionamiento, la entidad de certificación notificará a la autoridad competente lo antes posible y asegurará que los certificados válidos en el momento del cese de la actividad o han sido traspasados a otra entidad de certificación o invalidados.
(2) Se entregará la documentación según el Nº 10 a la entidad de certificación que tomará posesión de los certificados, o en todo caso a la autoridad competente.

(3) Se notificará a la autoridad competente, sin retraso indebido, de una petición de insolvencia, o una petición para el inicio de procedimientos concúrsales."

j. Protección de datos

1) "La entidad de certificación sólo puede recoger datos personales directamente de la parte involucrada, y cuando sean requeridos para los propósitos de un certificado. La recogida de datos de terceras partes sólo se permitirá con el consentimiento de la parte involucrada.

2) Donde el propietario de una clave de firma utilice un seudónimo, la entidad de certificación estará obligada a comunicar, bajo petición, a las personas involucradas cualquier dato relacionado con su identidad que sea requerido para el procesamiento de infracciones criminales o administrativas, para la prevención de peligro al orden o seguridad pública o para el cumplimiento de deberes estatales por la autoridad federal y estatal para la protección de la constitución, el Servicio de Inteligencia Federal, el Servicio de Contraespionaje Militar o la Oficina Criminológica de Aduanas. Tales

revelaciones serán documentadas. La autoridad solicitante informará al propietario de la clave acerca de la revelación del seudónimo, en tanto que no interfiera en el cumplimiento de sus deberes legales o cuando el propietario de la clave de firma tiene un interés primordial en que le den tal información.

(3) Nº 38 de la Ley de Protección Federal de Datos solicitará la condición de que la verificación pueda también ser realizada cuando no hay indicación de violación o estipulación de protección de datos."

k. Control y aplicación de obligaciones.

"1. La autoridad competente puede tomar medidas contra las entidades de certificación para asegurar la conformidad con este Decreto y la Ordenanza que tiene fuerza de ley. En particular, puede prevenir el uso de componentes técnicos inadecuados y puede prohibir temporalmente el funcionamiento de la autoridad de certificación totalmente o en parte. Las partes que tengan una licencia de acuerdo con el N° 4, sin ser éste el caso, se les puede prohibir realizar su actividad de certificación.

Para las intenciones de supervisión de acuerdo con (1) frase 1 acerca de que las autoridades de certificación permitirán a la autoridad competente entrar en los lugares de producción y locales de negocios durante horas de trabajo normales, bajo la petición de hacer válidos para inspección cualquier libro relevante, registros, documento de soportes, papeles y cualquier otra documentación, revelará información y proveerá de todo el soporte necesario.

Cualquiera que esté obligado a dar información puede rehusar responder preguntas que le perjudiquen a él o a una persona relacionada por afinidad de sangre, tal y como se especifica en Nº 3113 (1) Nº 1 a 3 del Código de Procedimiento Civil responsable de procesar o proceder bajo la ley de infracciones administrativas. Cualquier persona obligada a responder preguntas será avisada de este derecho.

(1) En caso de no cumplimiento de las obligaciones resultantes de este Decreto o la ordenanza que tiene fuerza de ley o en caso de que haya una razón para denegar una licencia, la autoridad competente revocará la licencia otorgada cuando es improbable que las medidas de acuerdo con Nº 13 (1) frase puedan no prosperar.

(2) En caso de retirada o revocación de una licencia o cese del funcionamiento de una entidad de certificación o terminará los contratos con los propietarios de las claves de firma. También se aplicará cuando una petición de insolvencia o una petición de por la institución de procedimientos de composición esté archivada y la actividad autorizada sea discontinua.

(3)La validez de los certificados expedidos por una entidad de certificación permanecerá no afectada por la retirada o revocación de una licencia. La autoridad competente puede ordenar la invalidez de certificados, cuando los hechos justifican la suposición de que los certificados han sido falsificados has sido falsificados o no están totalmente protegidos contra falsificación, o cuando los componentes técnicos utilizados para las claves de firmas revelan defectos en la seguridad, que permiten que firmas digitales sean falsificadas o que datos importantes sean manipulados sin poder detectarlos."

I. Componentes técnicos

(1) "Se necesitan componentes técnicos protegidos para la generación y almacenamiento de claves de firma y para la creación y verificación de firmas digitales que revelan con certeza firmas digitales falsificadas y datos manipulados y suministran protección contra el uso no autorizado de claves privadas de firma.

(2) Se necesitan componentes técnicos protegidos para la presentación de datos ser firmados que claramente indican de antemano la creación de una firma digital y permiten la identificación de los datos a los que la firma digital se aplica.

(3) Se necesitan componentes técnicos protegidos para la verificación de firmas digitales. Esto es, comprobar la integridad de los datos a los que se asocia esta firma digital y comprobar la identidad del propietario de la clave de firma utilizada.

(4) Los componentes técnicos que permiten mantener disponibles los certificados de clave de firma para la verificación o recuperación de acuerdo con Nº 5 (1) frase 2 requieren mecanismos de seguridad para proteger las listas de certificados contra alteraciones y recuperaciones no autorizadas.

(5) Los componentes técnicos referidos en Nº 14 (1) a (3) serán adecuadamente comprobados según los estándares de ingeniería existentes y su conformidad con los requisitos deberá ser confirmada por un organismo reconocido por la autoridad competente.

(6) Los componentes técnicos manufacturados legalmente o situados en el mercado con regulaciones o requerimientos en vigor en otro estado que sea miembro de la Unión Europea o en otro Estado perteneciente al Acuerdo del Espacio Económico Europeo que asegure el mismo nivel de seguridad se asumirá que cumple los requisitos técnicos de seguridad conformes con Nº 14 (1) a (3). En una instancia justificada y en solicitud de la autoridad competente se proporcionará prueba de conformidad de los requisitos referidos en el párrafo 1.

En tanto que se requiere la presentación de una confirmación por un organismo reconocido por la autoridad competente como evidencia de conformidad con los requisitos técnicos de seguridad referidos en Nº 14 (1) a (3), las confirmaciones por organismos con licencia en otros Estados miembros de la Unión Europea u otros estados pertenecientes al Acuerdo Del Espacio Económico Europeo también se aceptarán si los requisitos técnicos, pruebas y procedimientos de pruebas sobre los que los informes de pruebas de estos organismos están basados, son considerados equivalentes a aquellos de los organismos reconocidos por la autoridad competente."

m. Certificados expedidos por otros países

(1) "Las firmas digitales capaces de ser comprobadas por una clave pública de firma certificada en otro Estado Miembro de la Unión Europea o en otro Estado perteneciente al Acuerdo del Espacio Económico Europeo se consideran equivalentes a las firmas digitales bajo este Decreto mientras que muestren el mismo nivel de seguridad.

(2) El párrafo (1) también se aplicará a otros Estados cuando relevantes acuerdos supranacionales o intergubernamentales se hayan llevado a cabo."

n. Decreto

"El Gobierno Federal tendrá potestad para emitir, mediante Decreto con Fuerza de ley estipulaciones legales requeridas para la ejecución de $ 33 a 15 con respecto a:

1. Más detalles sobre el procedimiento relativo a la concesión, retirada o revocación de una licencia y el procedimiento sobre el cese del funcionamiento de una entidad de certificación.

12. Servicios tarificables de acuerdo al Nº 4 (6) y el nivel de la cuota.

3. Más detalles sobre las obligaciones de las entidades de certificación.

4. Períodos de validez de los certificados de clave de firma.

5. más detalles sobre el control de las entidades de las entidades de certificación.

6. Requisitos detallados aplicables a componentes técnicos, su comprobación y confirmación de conformidad con los requisitos.

7. El período tras el que una nueva firma digital debería analizarse, y el procedimiento utilizado.

F. LEY 2000-230 SOBRE LA ADAPTACIÓN DEL DERECHO DE LA PRUEBA A LAS NUEVAS TECNOLOGÍAS DE LA INFORMÁTICA Y RELATIVA A LA FIRMA ELECTRÓNICA EN FRANCIA (JOURNAL OFFICIEL DE LA REPUBLIQUE FRANCOISE DEL 14 DE MARZO DE 2000)

La Asamblea Nacional y el Senado han adoptado,

El Presidente de la República promulga la ley cuyo tenor dice:

ARTÍCULO 1.

I. El artículo 1316 del Código Civil pasa a ser el artículo 1315-1.
II. Los parágrafos 1º, 2, 3, 4 y 5 de la Sección I, del capitulo VI del Titulo III del Libro III del Código Civil pasan a ser los parágrafos 2,3,4,5, y 6 respectivamente.
III. Se inserta antes del parágrafo II de la sección I del capítulo VI del título III del libro tercero del Código Civil, un parágrafo I titulado Disposiciones generales, que comprende los artículos 1316 a 1316-2 así redactados.

ARTÍCULO 1316.

La prueba literal, o prueba por escrito, resulta de una sucesión de letras, de caracteres, de cifras o de todo otro signo o símbolo dotado de una significación inteligible, cualquiera que sea su soporte y sus modalidades de transmisión.

ARTÍCULO 1316-1.

El documento en forma electrónica se admite como prueba en las mismas condiciones que el documento en soporte papel, a condición de que pueda ser debidamente identificada la persona de la que emana y que sea aportado y conservado en las condiciones de naturaleza que garanticen su integridad.

ARTÍCULO 1316-2.

Mientras la ley no fije otros principios, y a falta de pactos válidos entre las partes, el juez dirimirá los conflictos de prueba literal determinando por cualquier medio el título más idóneo, cualquiera que sea el soporte.

ARTÍCULO 2.

El artículo 1317 del Código Civil se completa por un párrafo así redactado:

Se puede dirigir en soporte electrónico sí está establecido y conservado en las condiciones fijadas por Decreto del Consejo de Estado.

ARTÍCULO 3.

Después del artículo 1316-2 del Código Civil se inserta un artículo 1316-3, así redactado:

ARTÍCULO 1316-3.

El documento en soporte electrónico tiene la misma fuerza probatoria que el documento en soporte papel.

ARTÍCULO 4.

Después del artículo 1316-3 del Código Civil, se inserta el artículo 1316-4 así redactado:

ARTÍCULO 1316-4.

La firma necesaria para la perfección de un acto jurídico identifica a aquel que la pone. Ella manifiesta el consentimiento de las partes a las obligaciones que derivan de tal acto. Cuando la emite un funcionario público, la firma confiere autenticidad al acto.
Cuando sea electrónica, consiste en el uso de un procedimiento fiable de identificación garantizando su correspondencia con el acto al que se adjunte.
La fiabilidad de este procedimiento se presumirá salvo prueba en contrario, mientras la firma electrónica sea creada, la identidad del signatario asegurada, y la integridad del acto garantizada, en las condiciones fijadas por Decreto del Consejo de Estado.

ARTÍCULO 5.

En el artículo 1326 del Código Civil, las palabras de su mano se reemplazan por las palabras por él mismo.

ARTÍCULO 6.

La presente ley es aplicable en Nueva Caledonia, en la Polinesia Francesa, en Wallis-et-Futuna y en el Conjunto Territorial de Mayotte.

La presente ley será ejecutada como ley del Estado.
Hecha en Paris, el 13 de marzo de 2000 Jacques Chirac.

D. DECRETO Nº 513 DE 10 DE NOVIEMBRE DE 1997, EN ITALIA

(GACETA UFFICIALE DEL 13 DE MARZO DE 1998, Nº 60).

Reglamento relativo a los criterios y modalidades para la formación, el archivo y la transmisión de documentos con instrumentos informáticos y telemáticos, en virtud del artículo 15, párrafo 2º de la ley 15 de marzo 1997,Nº 59

El Presidente de la República

Visto el artículo 87 de la Constitución, visto el artículo 17, párrafo 2º de la Ley de 23 de agosto de 1988, Nº 400;

Visto el artículo 15, párrafo 2, de la ley de 15 de marzo de 1997, Nº 59.

Visto el Decreto Legislativo de 12 de febrero de 1993, Nº 39.

Oído el Garante para la protección de los datos personales;

Vista la deliberación preliminar del Consejo de Ministros, adoptada en la reunión del 5 de agosto de 1997;

Alcanzado el visto bueno de las comisiones permanentes de la Cámara de Diputados y del Senado de la República;

Escuchada la opinión del Consejo de Estado, expresando en la sección consultiva para los actos normativos en la audiencia del 20 de octubre de 1997;

Vista la deliberación del Consejo de Ministros, adoptada en la reunión del 31 de octubre de 1997;

Sobre la propuesta del Presidente del Consejo de Ministros y del Ministro para la función pública y los asuntos regionales, de conformidad con el Ministro de gracia y justicia;

Emana el siguiente reglamento:

a. Principios generales.

Definiciones.

ARTÍCULO 1.

1. " A los fines del presente reglamento se entiende por:

a) Por documento informático, la representación informática de actos, hechos o datos jurídicamente relevantes;

b) Por firma digital el resultado del procedimiento informático (validación) basado sobre un sistema de claves asimétricas por parejas, una pública y una privada que permite al firmante a través de la clave privada y al destinatario a través de la clave pública, respectivamente, manifestar y verificar el origen y la integración de un documento informático;

c) Por sistema de validación, el sistema informático y criptográfico capaz de generar e insertar la firma digital o de verificar su valides;

d) Por claves asimétricas, la pareja de claves criptográficas, una privada y una pública, relacionadas entre ellas, para utilizarlas en el ámbito de los sistemas de validación o de cifrado de documentos informáticos;

e) Por clave privada, el elemento de la pareja de claves asimétricas destinado a ser conocido solamente por el sujeto titular, mediante el cual ser inserta la firma digital sobre el documento informático o se descifra el documento informático previamente cifrado mediante la correspondiente clave pública;

f) Por clave pública, el elemento de la pareja de claves asimétricas destinado a ser público, con el cual se verifica la firma digital inserta en el documento informático del titular de las claves asimétricas o se cifran los documentos informáticos a transmitir al titular de las claves anteriormente citadas;

g) Por clave biométrica, la secuencia de códigos informáticos utilizados en el ámbito de mecanismos de seguridad que emplean métodos de verificación de la identidad personal basados en características físicas especificas del usuario;

h) Por certificación, el resultado del procedimiento informático, aplicado a la clave pública y reemplazable por los sistemas de validación, mediante la cual se garantiza la correspondencia biunívoca entre la clave pública y sujeto titular al cual ésta pertenece, se identifica este último y se atestigua el período de validez de la citada clave y el término de vencimiento del relativo certificado, en cualquier caso no superior a tres años;

i) Por validación temporal, el resultado del procedimiento informático, con el que se atribuyen a uno o más documentos informáticos, una fecha y una hora oponibles a terceros;

j) Por dirección electrónica, el identificador de un recurso físico o lógico capaz de recibir y registrar documentos informáticos.

k) Por certificador, el sujeto público o privado que efectúa la certificación, emite el certificado de la clave pública, lo publica conjuntamente a ésta última, publica y actualiza las listas de los certificados suspensos y revocados;

l) Por revocación del certificado, la operación con la cual el certificador anula la validez del certificado a partir de un determinado momento, no retroactivo, en adelante;

m) Por suspensión del certificado, la operación con la cual el certificador suspende la validez del certificado por un determinado período de tiempo;

n) Por validez del certificado, la eficacia y la oponibilidad al titular de la clave pública, de los datos en él contenidos;

o) Por normas técnicas, las específicas de carácter técnico, incluyendo toda disposición que sea aplicable."

b. Documento informático.

ARTICULO 2

1. "El documento informático quienquiera que lo forme, el archivo en soporte informático y la transmisión con instrumentos telemáticos, son válidos y relevantes a todos los efectos de ley si son conformes con las disposiciones del presente reglamento."

c. Requisitos del documento informático.

ARTICULO 3.

1. "Con decreto del Presidente del Consejo de Ministros, que se emanará en los ciento ochenta días siguientes a la fecha de entrada en vigor del presente reglamento, oída la Autoridad para la informática de la Administración Pública se fijarán las normas técnicas para la formación, la transmisión, la conservación, la duplicación, la

reproducción y la validación, también temporal, de los documentos informáticos.

2. Las normas técnicas indicadas en el párrafo 1° se adecuarán a las exigencias dictadas por la evolución de los conocimientos científicos y tecnológicos, con el transcurso de al menos dos años a partir de la de la de entrada en vigor del presente reglamento.

3. Con el decreto mencionado en el párrafo 1° también se dictarán medidas técnicas, organizativas y de gestión destinadas a garantizar la integridad, la disponibilidad y el secreto de las informaciones contenidas en el documento informático también referentes al uso hipotético de claves biométricas.

4. Se mantiene todo lo previsto en el artículo 15 de la ley de 31 de diciembre de 1996, N° 675."

d. Forma escrita.

ARTICULO 4.

1. "El documento informático que reúna los requisitos previstos por el presente reglamento satisface el requisito legal de la forma escrita.
2. Las obligaciones fiscales relativas a los documentos informáticos y a su reproducción en distintos tipos de soportes se cumplirán sobre la base de las modalidades definidas mediante decreto del Ministerio de Finanzas."

e. Eficacia probatoria del documento informático.

ARTICULO 5.

1. "El documento informático, rubricado con firma digital en el sentido del artículo 10, tiene la eficacia de escritura privada en el sentido del artículo 2702 del Código Civil.

2. El documento informático que reúna los requisitos previstos por el presente reglamento tiene la eficacia probatoria prevista en el artículo 2712 del Código Civil y satisface la obligación prevista por los artículos 2214 y siguientes del Código Civil y satisface la obligación prevista por los artículos 2214 y siguientes del Código Civil y de cualquier otra disposición legislativa o reglamentaria análoga."

f. Copias de actos y documentos.

ARTICULO 6. "1. .Los duplicados, las copias, los extractos del documento informático, incluso sin son reproducidos en distintos de soporte, son válidos y relevantes a todos los efectos de la ley si son conformes a las disposiciones del presente reglamento.

2. Los documentos informáticos que contienen copia o reproducción de actos públicos, escrituras privadas y documentos en general, incluyendo los actos y documentos administrativos de todo tipo, expedidos o emitidos por los depositarios públicos autorizados y de los funcionarios públicos, tienen plena eficacia, en el sentido de los artículos 2714 y 2715 del Código Civil, si a ellos se inserta o asocia la firma digital de aquél que lo envía o emite, según las Disposiciones del presente reglamento.

3. Las copias en soporte informático de documentos, formados originalmente en soporte papel o, en cualquier caso, no informático, sustituyen, a todos los efectos de la Ley, los originales de los que se trate si su conformidad con el original se autentica por un notario o por otro funcionario público autorizado, con declaración adjunta al documento informático y conformadas con las modalidades indicadas en el decreto mencionado en el párrafo 1 del artículo 4.

4. El envío o emisión de copias de actos y documentos del párrafo 2ª exonera de producción y de la exhibición del formato original en soporte de papel cuando se solicite a todos los efectos de ley.

5. Las obligaciones de conservación y exhibición de los documentos previstos por la legislación vigente se entienden satisfechas a todos los

efectos de ley por medios informáticos, si los procedimientos utilizados son conformes a las normas técnicas dictadas en virtud del artículo 3."

g. Deposito de la clave privada.

ARTICULO 7

1. El titular de la pareja de claves asimétricas puede obtener el depósito en forma secreta de la clave privada a través de un notario u otro depositario publico autorizado.

2.- La clave privada de la que se precisa el depósito puede ser registrada en cualquier tipo de soporte idóneo a cargo del depositante y debe ser entregada cerrada en un sobre lacrado de tal modo que la información no pueda ser leída, conocida o extraída sin roturas o alteraciones.

3.- Las modalidades del depósito se regulan por las disposiciones del artículo 605 del Código Civil en todo lo que sean de aplicación.

h. Certificación.

ARTICULO 8

"1.- Quien pretenda utilizar un sistema de claves asimétricas de cifrado con los efectos del artículo 2 deberá disponer de una pareja de claves idónea y hacer publica una de ellas mediante el procedimiento de certificación.

2.- Las claves publicas de cifrado se guardaran por un periodo no inferior a diez años por parte del certificador y a partir del momento inicial de su validez, son consultables en forma telemática.

3.- Salvo lo previsto por el artículo 17, las actividades de certificación se efectúan por certificadores incluidos, sobre la base de una declaración anterior al inicio de la actividad, en listas publicas especificas, consultables por vía telemática, mantenidas y actualizadas por la autoridad para la informática en la administración publica, y dotadas de los siguientes requisitos, especificados en el Decreto mencionado en el artículo 3:

a) Forma de Sociedad Anónima y capital social no inferior al necesario para la autorización para la actividad bancaria, si son sujetos privados.

b) Posesión por parte de los representantes legales y de los sujetos que la administren, de los requisitos de honorabilidad requeridos para los sujetos que desarrollan funciones de administración, dirección y control en los bancos.

c) Confianza que, por competencia y experiencia , los responsables técnicos del certificador y el personal encargado de la actividad de certificación sean capaces en grado de respetar las normas del presente reglamento y las normas técnicas a las que alude el artículo 3.

d) Cualidad de los procesos informáticos y de los productos relacionados, sobre la base de los estándares reconocidos a nivel internacional.

4.- El procedimiento de certificación del párrafo 1 puede ser desarrollado también por un certificador que opere sobre la base de una licencia o autorización emitida por otro Estado Miembro de la Unión Europea o del Espacio Económico Europeo, en virtud de requisitos equivalentes."

i. Obligaciones del usuario y del certificador.

ARTICULO 9.

"1. - Quien pretenda utilizar un sistema de claves asimétricas o de la firma digital, está obligado a adoptar todas las medidas organizativas y técnicas idóneas para evitar daños a otros.

2. - El certificador está obligado a:

a) Identificar con certeza la persona que hace la solicitud de certificación.

b) Emitir y hacer público el certificado que contenga las características fijadas con el Decreto del artículo 3.

c) Especificar, sobre la solicitud del solicitante, y con el consentimiento del tercero interesado, la subsistencia de los poderes de representación o de los otros títulos relativos a la actividad profesional o a los cargos desempeñados.

d) Atenerse a las normas técnicas del artículo 3.

e) Informar a los solicitantes, de manera cumplida y clara, sobre el procedimiento de certificación y sobre los requisitos técnicos necesarios para acceder.

f) Atenerse a las medidas mínimas de seguridad para el tratamiento de los datos personales emanados en virtud del artículo 15, párrafo 2 de la ley de 31 de diciembre de 1996, N°. 675.

g) No ser depositario de claves privadas.

h) Proceder tempestivamente a la revocación o suspensión del certificado en caso de solicitud por parte del titular o del tercero del cual se deriven los poderes de éste último, de pérdida de la posesión de la clave, de disposición de la autoridad, de adquisición del conocimiento de causas limitativas de la capacidad del titular, de sospechas de abuso o falsificaciones.

i) Dar publicación inmediata de la revocación y de la suspensión de la pareja de claves asimétricas.

j) Comunicar inmediatamente a la autoridad para la informática en la Administración Pública y a los usuarios, con un preaviso de al menos seis meses, de la cesación de la actividad y de la consiguiente transmisión de la documentación a otro

k) certificador o de su anulación."

j. Firma digital.

ARTICULO 10.

"1. A cada documento informático, o a un grupo de documentos informáticos, y al duplicado o copia de ellos, puede insertarse o asociarse con una evidente separación informática, una firma digital.

2. La inserción o asociación de la firma digital al documento informático equivale a la firma prevista para los actos y documentos en forma escrita en soporte de papel.

3. La firma digital se debe referir de manera unívoca a un solo sujeto y al documento o conjunto de documentos a los que se inserta o asocia.

4. Para la generación de la firma digital debe emplearse una clave privada cuya correspondiente clave pública no esté caducada o haya sido revocada o suspensa por el sujeto público o privado que la ha certificado.

5. El uso de la firma adjunta o asociada mediante una clave revocada, caducada o suspensa equivale a la falta de firma. La revocación o la suspensión, en todo caso motivada, tienen efecto desde el momento de la publicación, salvo que el revocante, o quien solicite la suspensión, no demuestre que ésta era ya conocida por todas las partes interesadas.

6. La inserción de firma digital integra y sustituye a todos los fines previstos por la normativa vigente, los distintivos con lacre, punzones, sellos, contraseñas y marcas de cualquier tipo.

7. A través de la firma digital se deben poder transmitir, en los modos y con las técnicas definidas con el decreto mencionado en el artículo 3, los elementos identificativos del sujeto titular de la firma, del sujeto que la ha certificado y del registro en el que ésta esta publicada para su consulta."

k. Contratos celebrados con medios informáticos o por vía telemática.

ARTICULO 11

"1. Los contratos celebrados con medios informáticos o por vía telemática mediante utilización de la firma digital según las disposiciones del presente reglamento es válida y relevante a todos los efectos de ley.

2.- A los contratos mencionados en el párrafo 1 se le aplican las disposiciones previstas en el Decreto Legislativo de 15 de enero de 1992, número 50."

l. Transmisión del documento.

ARTICULO 12..

"1. El documento informático transmitido por vía telemática se entiende enviado y recibido por el destinatario si se transmite a la dirección electrónica declarada.

2. La fecha y hora de formación, transmisión y recepción de un documento informático, redactado de conformidad con las disposiciones del presente reglamento y a las normas técnicas a que hace referencia, el artículo 3, son oponibles a terceros.

3. La transmisión del documento informático por vía telemática, con las modalidades que aseguren la consabida entrega, equivale a la notificación por correo postal en los casos permitidos por la ley."

m. Firma digital autenticada.

ARTICULO 16.

"1. Se entiende reconocida, en el sentido del artículo 2073 del Código Civil, la firma digital, cuya anexión esté autenticada por un notario o de otro funcionario público autorizado.

2. La autenticación de la firma digital consiste en atestiguar, por el funcionario público, que la firma digital se adjunta en su presencia por el titular, previa comprobación de su identidad personal, de la valides de la clave utilizada y del hecho de que el documento firmado responda a la voluntad de la parte y no es contrario al ordenamiento jurídico en el

sentido del artículo 28, párrafo primero, número 1, de la ley de 16 de febrero de 1913, Nº 89.

3. La inserción de la firma digital por parte del funcionario público integra y sustituye, a todos los fines de la ley los distintivos con lacre, punzones, sellos, contraseñas y marcas previstas en todo caso.

4. Si el documento informático autenticado le debe ser adjuntado otro documento formado en su origen en otro tipo de soporte, el funcionario público puede adjuntar copia informática autenticada del original, según las disposiciones previstas en el artículo 6 del presente reglamento.

5. A los fines y para los efectos del artículo 3, párrafo 11 de la ley del 15 de mayo de 1997 núm. 127, se considera ajunta en presencia del dependiente encargado de la firma digital inserta en el documento informático presentado o depositado en las Administraciones Públicas.

6. La presentación o el depósito de un documento por vía telemática o en soporte informático en una administración pública es valida a todos los efectos de la ley si se inserta la firma digital y la validación temporal en virtud del presente reglamento".

n. Claves de cifrado de la administración pública.

Articulo 17.

"1. Las Administraciones Públicas actúan autónomamente, con referencia al propio ordenamiento, a la generación, conservación, certificación y utilización de las claves públicas de su competencia.
Con el decreto mencionado en el artículo 3 se establecen las modalidades de formación, de publicidad, conservación y de utilización de las claves públicas de las Administraciones Públicas.

2- Las claves públicas de los funcionarios públicos no pertenecientes a la Administración Pública son certificadas y publicadas autónomamente de conformidad con las leyes y los reglamentos que definen el uso de las firmas autógrafas en el ámbito de los respectivos ordenamientos jurídicos.

3- Las claves públicas de órdenes y colegios profesionales reconocidos y de sus representantes legales son certificados y publicados por parte del Ministerio de Gracia y Justicia o de sus delegaciones".

Ñ. Documentos informáticos de las administraciones públicas.

ARTICULO 18.

"1. Los actos formados con instrumentos informáticos, los datos y los documentos informáticos de las Administraciones Públicas, constituyen información primaria y original de la que es posible efectuar, sobre distintos tipos de soporte, reproducciones y copias para los usos consentidos por la ley.

2. En las operaciones relativas a las actividades de producción, introducción, archivo, reproducción y transmisión de datos, documentos y actos administrativos con sistemas informáticos y telemáticos, donde comprenda la emisión de los actos con los mismos sistemas, deben ser indicados y hechos fácilmente individualizables sea los datos relativos a las administraciones interesadas, sea el sujeto que ha realizado la operación.

3. Las normas técnicas en materia de formación y conservación de documentos informáticos de las Administraciones Públicas son definidas por la autoridad para la informática en la Administración Pública, de interés con la administración de los archivos de Estado y, por material clasificado, con las Administraciones de Defensa, Interior y Hacienda, respectivamente competentes".

o. Firma de los documentos informáticos de las administraciones publicas.

ARTICULO 19.

"1.- En todos los documentos informáticos de las Administraciones Públicas la firma autógrafa, o la firma en todo caso prevista, se sustituye por la firma digital, de conformidad con las normas del presente reglamento.

2.- El uso de la firma digital integra y sustituye a todos los fines previstos por la ley, los distintivos con lacre, punzones, sellos, contraseñas y marcas de cualquier tipo".

Con posterioridad a la ley el 8 de febrero de 1999, se dicto el Decreto del Presidente del Consejo de Ministros, según gaceta oficial del 15 de abril 1999, cuya finalidad es establecer las normas técnicas para la formación, la transmisión, la conservación, la duplicación, la reproducción y la validación, también temporal, de los documentos informáticos en el sentido del articulo 3, párrafo 1, del decreto del Presidente de la Republica de 10 de noviembre de 1997, Nº 513 y también las citas medidas técnicas, organizativas y de gestión mencionadas en el articulo 3, párrafo 3, del mismo decreto del Presidente de la Republica de 10 de noviembre de 1997, Nº 513.

CONCLUSIONES

La problemática que se presenta con la admisibilidad y valoración de los documentos electrónicos en juicio, en los casos en que la ley nada dice, debe ser resuelta decididamente, pero con prudencia. Abordar en forma directa el tema del documento electrónico como medio de prueba, su valor y la validez de las firmas digitales y electrónicas, permitiría que el Juez adopte una actitud distinta frente a su presentación en juicio, al sentirse respaldado para admitirlo y valorarlo, ya que estaría tratando con un medio de prueba legal expreso.

Creemos necesaria una reforma a la legislación civil que admita las modalidades de pruebas que se citan en la actual ley procesal penal, más todos aquellos medios técnicos que correspondan al concepto amplio de documento.

Sin embargo, previamente conviene analizar, la naturaleza, características, ámbito de operación y las realidades propias de cada uno de los documentos en soporte papel que se reemplacen por uno magnético, al momento de adoptar modificaciones.

Sin perjuicio de lo anterior, mientras estas respuestas no lleguen, creemos que existen vías procesales para hacer valer en juicio los documentos electrónicos.

Se incluye el siguiente desarrollo a fin de esclarecer ciertas cuestiones relativas a la terminología de firma digital.

En primer lugar corresponde hablar de firma digital y no de firma electrónica, vocablo éste último que se utiliza erróneamente en nuestra legislación así como en otras legislaciones para referirse a la firma mecanizada para los fines de su procesamiento informático y que conste más de dígitos binarios y no de electrones.

Aunque es cierto que los dígitos de una firma digital consisten en magnitudes eléctricas cuando la firma digital se encuentra momentáneamente almacenada en la memoria volátil de un *PC ("RAM")*, también es cierto que cuando se encuentra almacenada en un disco duro (magnético) *de PC* consiste en campos magnéticos cuando se encuentra perdurablemente almacenada en un *CD-ROM* ,consiste en agujeros perforados en la capa de aluminio del *CD* y cuando es transmitida por una fibra óptica de telecomunicaciones consiste en fotones.

Lo que también es cierto es que en todas estas modalidades diferentes de almacenamiento y transmisión la firma mecanizada no pierde su cualidad numérica, es decir, digital, por lo que le corresponde su denominación como tal.

Se expone el presente argumento sin perjuicio de que el vocablo "firma digital" se corresponda mejor con la marcada tendencia internacional de la "digitalización" de la economía que el vocablo "firma electrónica".

También corresponde explicar que la firma digital sub-examine nada tiene que ver con la firma escaneada, es decir con el documento de procesador de palabras al cual se le ha anexado al pie la imagen escaneda de una firma manuscrita. La firma escaneada carecerá siempre de valor jurídico, pues por una parte quien recibe en disquete un documento que contiene la imagen escaneda de una firma manuscrita queda en total libertad de modificar el contenido de ese documento, y por la otra, cualquier persona puede escanear la firma manuscrita de otra y aplicarla al pie de un documento que cree con el contenido a su gusto.

Aunque parezca superfluo, conviene también explicar que la firma digital nada tiene que ver con la utilización de la impresión dactilar (ejemplo del

pulgar) utilizando una almohadilla de tinta, al pie de un documento en soporte papel.

Establecido ya que la información a la cual se le desea otorgar valor jurídico es digital, o sea numérica (binaria) conviene precisar la naturaleza de los posibles mecanismos disponibles para otorgarle validez jurídica a esa información numérica.

En este sentido cabe aseverar en forma axiomática y tautológica que el mecanismo de firma digital debe ser criptográfico, pues si lo que se desea es proteger la información, o sea los dígitos, se incursiona necesariamente en el campo de la criptografía, la que se define como el arte de proteger la información, tanto como para proteger su privacidad como para proteger su integridad. El término criptografía proviene del griego (Cristo: oculto) y es definido por el diccionario de la Real Academia como el "arte de escribir con clave secreta o de un modo enigmático" (Diccionario de la Lengua Española, Real Academia Española, vigésimo primera edición, Tomo I, Pág. 596, Madrid, 1992).

No se dice que el mecanismo de firma digital deba ser únicamente criptográfico, sino meramente que la criptografía forma parte esencial *sine*

qua non de ese mecanismo de firma digital, pudiendo intervenir en el proceso de firma otros mecanismos tales como los mecanismos biométricos, pero sólo en forma adicional a la criptografía.

Estableciendo que el mecanismo de firma digital es necesariamente criptográfico, conviene analizar qué mecanismos criptográficos son considerados aceptables, y cuáles no.

Como se expuso en el análisis previo de la firma manuscrita, una de las cualidades esenciales para que la misma tenga validez jurídica es que no sea fácilmente falsificable por un tercero, es decir, que existan garantías de que esa firma pueda ser creada sólo por una persona y no por otra.

En el ámbito informático y digital es posible reproducir cualquier información binaria, tal que la copia no es diferenciable de su original. Como ya se mencionó, esta es una de las razones por la que la firma manuscrita escaneada (digitalizada) no puede obtener validez jurídica.

Resta hallar entonces en el ámbito digital aquello que le confiera unicidad a las firmas digitales creadas por una persona, o sea una condición que permita identificar al creador de una firma digital, teniendo en cuenta que

cualquier cualidad manifiesta a simple vista puede ser fácilmente copiada y transferida de un documento a otro.

La condición buscada está disponible y consiste en el secreto no compartido. El concepto en su esencia es muy simple: el creador de una firma digital posee un elemento que sólo él conoce y posee y que le permite crear firmas digitales tal que quién las verifica pueda establecer inequívocamente que al firmar el creador de la firma digital necesariamente tuvo posesión de ese elemento, pero sin requerir que el creador de la firma digital tenga que divulgar ese secreto, con lo que el secreto dejaría de serlo.

Ese mecanismo existe y en el ámbito de la criptografía se denomina criptografía asimétrica o criptografía de clave pública. La criptografía asimétrica utiliza dos claves diferentes pero íntimamente relacionadas, tal que lo que encripa una clave sólo puede ser desencriptado por la correspondiente otra clave, y no por una clave ajena a ese par.

El mecanismo matemático utilizado asegura además que conociendo la clave pública no se tiene información alguna sobre la correspondiente clave privada. Este mecanismo contrasta con la más tradicional criptografía simétrica que utiliza la misma clave para encriptar que para desencriptar un

texto, por lo que el destinatario del texto para poder leerlo necesariamente debe conocer la clave secreta utilizada para encriptar ese texto con lo que esa clave secreta deja de ser secreta. Por ello la criptografía simétrica solo sirve para otorgarle privacidad a la información pero no como tecnología de firma digital.

En la criptografía asimétrica, la clave del encriptado se denomina privada y es mantenida secreta por el firmante mientras que la otra clave relacionada (de desencriptado) se denomina clave pública y se da a conocer. Las firmas digitales creadas por el firmante utilizando su clave privada, son verificadas por el destinatario del documento con la correspondiente clave pública. El hecho de que una firma digital sea verificable por medio de una cierta clave pública implica necesariamente que esa firma fue creada por la correspondiente clave privada, que por definición, el firmante mantuvo secreta y nunca divulgó.

Es esencial para su validez jurídica que el mecanismo de firma digital contemple la utilización de un secreto no compartido por el creador de una firma digital pues es este secreto no compartido lo único que impide que un tercero falsifique su firma, y si un mecanismo de firma permite la falsificación, deja de ser confiable, y si no es confiable no es realmente un mecanismo de

firma. Esta seguridad de no falsificación es intrínseca a cualquier mecanismo de firma.

Por lo expuesto es claro que el requisito de implementar la firma digital únicamente mediante la criptografía asimétrica, más que un requisito es una particularidad que, como se demostró surge naturalmente de la naturaleza intrínseca del problema a resolver, que es como identificar al autor de un documento digital y establecer si dicho documento fue posteriormente modificado.

Como quedó demostrado la criptografía simétrica no se puede utilizar como mecanismo de firma digital, y como la criptografía si no es simétrica es asimétrica queda la criptografía asimétrica como la única alternativa para implementar la firma digital. De hecho el algoritmo de clave asimétrica más popular por un amplio margen es el denominado RSA en honor a sus inventores Ronald Rivest, Adi Shamir y Leonardo Adleman que lo desarrollaron en el Massachussets Institute Of. Teechnology de los EE.UU.en 1977. La criptografía asimétrica RSA tiene disponibles, por ejemplo, múltiples implementaciones en los navegadores y servicios más populares y gratuitos del *internet*, con una base establecida de usuarios de decenas de millones en los diferentes países del mundo.

El requisito de implementar la firma digital únicamente mediante la criptografía asimétrica tampoco es restrictivo ni tecnológica ni comercialmente, pues la criptografía asimétrica no es una tecnología ni un algoritmo especial y propietario, sino meramente una definición que abarca todo y cualquier algoritmo criptográfico que utilice una clave diferente para encriptar que para desencriptar, de los cuales existen por lo menos una treintena de algoritmos diferentes utilizables.

Después de todo lo expuesto, pensamos adecuado para no desperdigar normas reguladoras de la prueba en distintas leyes especiales, el establecer de modo general este medio probatorio en el Código de Procedimiento Civil, y limitar la prueba en ciertos casos.

Nos parece que se debe ampliar el concepto de prueba documental, para regular el valor probatorio de ciertos soportes de datos utilizados en la computación, siempre que reúnan las condiciones de inalterabilidad exigidas y salvo prueba en contrario. Existe una moderna concepción doctrinaria sobre el alcance de la noción de documento, la cual compartimos, donde se incluyen todas las cosas representativas o simbólicas, elaboradas con predisposición, intención o aptitud de expresar ciertos significados, según

resulta de la elaboración de procesalistas de reconocida seriedad (Carnelutti, Devis Echandía y otros).

Es así como el procesalista Devis Echandía (1984,197) sostiene que documento es:

> "Toda cosa susceptible de percepción sensorial y aprehensión mental que sirve de demostración histórica indirecta y representativa de un hecho cualquiera, pudiendo ser declarativo y representativo o únicamente representativo y estar expresado en cualquier elemento material, que sirva para fines representativos: papel, madera, tela, muro, película fotográfica o cinematográfica, cinta grabadora etc." Consideramos que los soportes informáticos caben dentro de esta concepción."

Por su parte José María López afirma que la instrumentación puede consistir en un escribir, un dibujar, un grabar y que los procedimientos técnicos pueden ser los más distintos, lo extraño o singular del procedimiento no desvirtuaría por sí solo el carácter documental de la inscripción.

Consideramos que en materia informática existen métodos sustitutivos de la firma para imputar la autoría de los datos elaborados electrónicamente. La verosimilitud convoca a las reglas de la sana crítica para la apreciación de la prueba, según el sistema adoptado por nuestra legislación procesal civil. La sana crítica judicial puede acudir a las presunciones legales o judiciales para

establecer la verosimilitud, pues son medios probatorios expresamente incluidos en el Código de Procedimiento Civil.

En apoyo a lo anterior se puede concluir que se deben aceptar, en principio y bajo ciertas condiciones de fidelidad, inalterabilidad y completividad, según las reglas de la sana crítica y con la salvedad de la prueba en contrario, las constancias de almacenamiento, registración, recuperación y reproducción indelebles obtenidos en los sistemas electrónicos de elaboración de datos. Es decir, que los diferentes elementos que componen los sistemas electrónicos de la informática pueden ser presentados como prueba en cuanto fuesen pertinentes para acreditar los hechos controvertidos.

En definitiva la eficacia de su fuerza de convicción está supeditada a la prudente y sana crítica del juez, pudiendo éste auxiliarse con peritaje de expertos, testimonio de terceros, presunciones, consultas científicas, técnicas etc.para corroborar la verosimilitud.

Nuestro Código de Procedimiento Civil en el artículo 395 contiene un criterio ampliatorio de los medios de prueba admisibles al señalar que son medios de prueba admisibles en juicio aquellos que determina el Código Civil, el presente código y otras leyes de la República.

También se encuentra manifestado ese criterio ampliatorio de la siguiente manera:

> "Pueden también las partes valerse de cualquier otro medio de prueba no prohibido expresamente por la ley y que consideren conducente a la demostración de sus pretensiones. Estos medios se promoverán y evacuarán aplicando por analogía las disposiciones relativas a los medios de prueba semejantes contemplados en el Código Civil, y en su defecto en la forma que señale el Juez."

Del anterior artículo se deduce que ese criterio ampliatorio de nuestros medios de prueba permite que el Juez pueda valorar la prueba del documento electrónico y la firma digital con el establecimiento de la sana crítica judicial, la cual inviste a los jueces de suficientes facultades para esclarecer la verdad valorando críticamente los elementos aportados por los litigantes.

De todo lo anterior, podemos concluir que existe la necesidad de sancionar normas que contemplen las pruebas examinadas y su eficacia, y mientras estas respuestas no lleguen, creemos que existen vías procesales para hacer valer en juicio los documentos electrónicos.

REFERENCIAS BIBLIOGRAFICAS

Acha, J. (1996). ***Situación actual de la informática y los datos personales***: Algunas reflexiones sobre la situación real de la LOARTAD. Revista de informática y derecho. España: Aranzadi.

Aguado, M. (1990). ***La Utilización de Sistemas Expertos para la Recuperación Documental Jurídica***. Congreso internacional de informática y derecho en los umbrales del tercer milenio. Buenos Aires.

Aguiar, A. (2000). ***Revisión Crítica de la Constitución Bolivariana,*** El Nacional. Caracas.

Aguilar, J. (1987). ***Derecho Civil. Personas.*** Manuales de Derecho. Católica Andrés Bello. Caracas.

Aldana, E. (1988). ***Sistemas de Informática Jurídica Documental para Colombia***. Bogotá: Juriscol.

Ale, R. y Cuellar, F. (1988). ***Teleinformática.*** Mexico: McGraw-Hill.

Alestuey., M. (1994). ***Apuntes sobre la perspectiva criminológica de los delitos informáticos en informática y Derecho.*** III Congreso iberoamericano de informática y derecho. España: Aranzadi.

Alexy, R. (1997). ***Teoría de los Derechos Fundamentales*** (Trad. E. Garzón y R. Zimmerling) Centro de Estudios Constitucionales. Madrid.

Almark, D. y otros (1988). ***Informática y Derecho. Aportes de la Doctrina Internacional.*** Madrid: Depalma.

Almark, D. y Molina E. (1996). ***Protección de datos personales y reforma constitucional en revista informática y*** **Derecho.** España: Aranzadi.

Alvarez, M. y otros (2000). ***La libertad informática; derecho fundamental en la Constitución venezolana en el nuevo Derecho constitucional venezolano,*** IV Congreso de derecho constitucional en homenaje al Dr. Humberto J. La Roche. Caracas: Universidad Católica Andrés Bello.

Álvarez, J. (1997). ***Delitos informáticos***.:Jornadas sobre marco legal y deontológico de la informática. España: Aranzadi.

Álvarez-C., J. (2000). ***La firma y el comercio electrónico en España. Comentarios a la legislación vigente.*** España: Aranzadi.

Azurmedi, A. (1997). ***Derecho de la información. Guía jurídica para profesionales de la información.*** Pamplona: EUNSA.

Baón, R. (1996). ***Visión general de la informática en el nuevo código penal en ámbito jurídico de las tecnologías de la información,*** Cuadernos de derecho judicial. Madrid.

Barriuso, C. (1996). ***Interacción del Derecho y la informática***. Madrid: Dykinson.

Barroso, P. (1987). ***El derecho a la información, primer derecho humano, en información y derechos humanos***, Pamplona: Innerarity y Vaz.

Bauzá, M. (2000). ***La protección jurídica de los datos personales y los servicios de información comercial y crediticia,*** en http://publicaciones.derecho.org/redi/No._07_febrero_de_1999/bauza2.

Bel., C. y Alfonso, L. (1992). ***Derecho de la información. Sujetos y Medios***. Madrid: Colex.

Beltramone, G. (1997). ***El Derecho en la era digital***. Argentina: Juris.

Benito, A.. (1982). ***Fundamentos de teoría general de la información.*** Madrid: Pirámide.

Bielsa, R. (1986). ***Recuperación de documentos jurídicos por medios automatizados***.. Milano: Dott Editore.

Brewer-C., A. (2000). ***La Constitución de 1999 comentada.*** Caracas: Arte.

Briceño, F., Muci, G. y Viloria, M. (1999). ***Comercio electrónico***: Algunos temas legales. Caracas: Andersen Legal.

Buitrago, D. (2002). ***El Derecho y la industria informática.*** Colombia: Señal

Cabanellas, G.(1989). ***Diccionario enciclopédico de derecho usual.*** Buenos Aire: Heliasta.

Cafure, M. (1995). **El delito informático en la agenda internacional.** España: Cuadernos de departamento de derecho penal y criminología. Universidad Nacional de Córdova.

Carrasco, H. (2000). **Contratación electrónica y contratos informáticos.** Santiago de Chile: La Ley.

Carreras, F. (1991). ***La libertad de expresión: un derecho constitucional, en libertad de expresión***. España: Departamento de Ciencia Política y Derecho Público de la Universidad Autónoma.

Capitant, H. (1981). ***Vocabulario jurídico.*** Buenos Aires: Depalma.

Carnelutti, F. (1982). **Teoría general del derecho. Editorial Revista de derecho privado.**

Consejo General de los Colegios Oficiales de Corredores de Comercio. (1999). **Firma electrónica y comercio electrónico.** Madrid. Dykinson,S.L.

correa, C. (1996). ***El derecho informático en América latina, en informática y derecho. aportes de doctrina internacional***. (Vol. 2). Buenos Aires: Depalma.

_____(1991). ***Evolución reciente del derecho informático en américa latina en la ley.*** Buenos Aires: A-893.

Cuadernos de derecho judicial. (2000). **Problemática jurídica en torno al fenómeno de internet**. Madrid:Lerko Print S.A.

Davara, M. (1997). ***Manual de derecho informático.*** Pamplona: Aranzadi.

Decreto con fuerza de Ley de mensaje de datos y firma electrónica (2001) ***Gaceta oficial de la Republica Bolivariana de Venezuela.*** Nº 37148. febrero 28 de 2001.

Delpiazzo, C. (1996). ***Evolución y perspectivas del tratamiento jurídico del sofware en América latina***. Revista informática y derecho. España: Aranzadi.

Espinosa, Aldo (1992). ***La justicia un reto de la informática en ciencia y tecnología***. (Vol. 6). Bogotá: Colciencias.

Espinosa, J. (1988). ***El Derecho Informatizado.*** Ibagué: Lopera.

Eugenio, F. y Eugenio, L. (1994). ***Protección de datos. análisis comparado de la legislación de algunos países europeos: Alemania, España, Francia y Gran Bretaña.*** IV Congreso iberoamericano de informática y derecho. Argentina.

Frosini, V. (1982). **Cibernética.** Conferencia en la Junior Bar Conferencia of de American Bar Association, en San Francisco California. Usa.

Garzón, G. (1981) ***El marco jurídico del flujo de datos transfronteras***,. Roma: IBI Doc, TDF 102.

Guasp, J. (1977). ***Derecho procesal civil,*** (3ra ed. 2° reimp.). Madrid.

Gustavino, E, (1987). **Responsabilidad civil y otros problemas jurídicos en computación.** Buenos Aires: Ediciones La Roca.

Gómez, M. (1994). **Los delitos informáticos en el derecho español. Informática y derecho.** España: Centro Regional de Extremadura

Guibourg, R. (1996). ***Manual de informática jurídica***. Buenos Aires: Astrea.

Hance, O. (1996). ***Leyes y negocios en internet.*** México: Mc Graw Hill.

Hernández, G (2000). ***La informática jurídica***. Colombia: Doctrina y Ley LTDA.

Jijena, R. (2002) .**Comercio electrónico, firma digital y derecho**. Chile: Jurídica de Chile.

Lazpita G., M. (1994). ***Análisis comparado de las legislaciones sobre protección de datos de los estados miembros de la comunidad europea.*** Revista informática y derecho. España: Aranzadi.

López-M. G. (1994). ***Los derechos de las personas en la ley de protección de datos personales***. Revista informática y derecho. España: Aranzadi.

Lucena. J. (1999). ***Criptografía y seguridad en computadores.*** http://www.kriptopolis.com.

Madrid, F. (1984) **Derecho a la intimidad informática y Estado de Derecho.** España: Universidad de Valencia.

Marín, L. (2000). **Los contenidos ilícitos y nocivos en internet**. Madrid: Fundación Retevision.

Martínez, A. (2001). **La ley de firma electrónica.** España: Gráficas Rogar.

Martinez, R. (1999). **Régimen jurídico de internet.** Buenos Aires: Ad-hoc

Mármol, H. (1978). ***Fundamentos del derecho mercantil.*** Caracas: Universidad Católica Andrés Bello.

Molina, J. (1996). ***Libertad informática y criptología.*** Revista de informática y derecho. España: Aranzadi.

Molinero, C. (Ed. 1989) ***Teoría y fuentes del derecho de la información***, Barcelona: Autor.

Natalio, C. (1997). ***Ciberespacio y derecho:*** Desafíos que el comercio electrónico plantea al derecho comercial tradicional, los contratos telemáticos, Revista de derecho. Buenos Aires.

Navalpotro, Y. (2001). ***Críticas a la nueva ley española de protección de datos personales.*** http://vlex.com/es/canales/Constitucional/Art@iculos/1.

Ortiz, R. (1992). **La vida privada el honor y la reputación. Criterios jurídicos para su definición y alcance.** Caracas: El greco

_____(2001).**Habeas data. Derecho fundamental y garantía de protección de los derechos de la personalidad.** Caracas: Fronesis.

Palazzi, P. (2000). ***Derecho y nuevas tecnologías***. Buenos Aires: Ad-Hoc

_____.2000).**Delitos Informáticos.** Buenos Aires Ad-Hoc.

Pérez, F. (1992). ***Computación y ética:*** II Jornadas sobre Derecho y computación celebradas en Cumaná. Caracas: Vadell hermanos.

Pietro, M. (1984). ***Informática jurídica***: El Derecho ante un gran reto. Bogota: Universidad Javeriana.

Real Academia Española (1884). ***Diccionario de la lengua española.*** Madrid: Espasa-Calpe.

Ribas, J. (Ed. 2000). ***Comercio electrónico en internet***: Problemática jurídica en torno al fenómeno de internet. Madrid: Autor.

Rivera, A. (1995), ***Dimensiones de la informática en el derecho***: perspectivas y problemas. Bogotá: Jurídicas Radar.

Rivera, R. (1995). **Dimensiones de la informática en el derecho.** Bogota: Ediciones jurídicas Radar.

Rocco, A.(1955). ***Principios de derecho mercantil.*** México: Nacional.

Sánchez, R. (1974). ***El Derecho a la información***. Bogotá: Cosmos.

Sánchez, J. y Cáceres, P. (1989). ***La Informática en el ámbito del derecho.*** Pontificia Universidad Javeriana. Bogotá.

Sánchez, M. (1993). ***La transparencia de las bases de datos como mecanismos de protección de la intimidad de las personas.*** Revista informática y derecho España: Aranzadi.

Sanchis, C. (1999). ***La prueba por soportes informáticos***, España: Tirant lo blanch.

Solano, O. (1997). ***Manual de informática jurídica.*** Bogotá: Ediciones jurídicas Gustavo Ibáñez.

Tiedemahn, K. (1985). **Poder económico y delito.** Barcelona: España.

Uwe K. y otros (1983). ***Las repercusiones sociales de la tecnología informática***. Madrid: Fundesco-Técnos.

Vargas, T. (1993). ***Manual de introducción a la informática jurídica***.. Bogota: Externado de Colombia.

Velásquez, R. (1993). ***Protección jurídica de datos personales automatizados***. Madrid: Colex

Tellez, J. (1996) **Los delitos informáticos. Situación en México**. Mérida: Centro Regional de Extremadura.