

146
2ej



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

EL DOCUMENTO ELECTRÓNICO
COMO FORMA DE CONTRATACIÓN

T E S I S

PARA OBTENER EL TÍTULO DE
LICENCIADO EN DERECHO.

P R E S E N T A

DURÁN MORA MÓNICA

ASESOR: LIC. PABLO A. PRUNEDA PADILLA



CIUDAD UNIVERSITARIA

1999

TESIS CON
FALLA DE ORIGEN



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE DERECHO
SEMINARIO DE DERECHO CIVIL

ING. LEOPOLDO SILVA GUTIERREZ
DIRECTOR GENERAL DE LA ADMINISTRACION ESCOLAR
DE LA UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
P R E S E N T E.

Muy distinguido señor director:

La pasante DURAN MORA, MONICA con número de cuenta 9450970-4, inscrita en el Seminario de Derecho Civil a mi cargo, ha elaborado su tesis profesional intitulada "EL DOCUMENTO ELECTRONICO COMO FORMA DE CONTRATACION", bajo el asesoramiento del Lic. Pablo A. Pruneda Padilla, para obtener el título de Licenciado en Derecho.

Por lo que con apoyo en los artículos 10 fracción VIII y demás relativos del vigente Reglamento de Exámenes Profesionales suplico a usted ordenar la realización de los trámites tendientes a la celebración del examen profesional de la pasante de referencia.

Asimismo, la interesada deberá iniciar el trámite para su titulación dentro de los seis meses siguientes (contados de día a día) a aquél en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que no deberá otorgarse nuevamente sino en el caso de que el trabajo recepcional conserve su actualidad y siempre que la oportuna iniciación del trámite para la celebración del examen profesional, haya sido impedida por circunstancia grave, todo lo cual lo calificará la Secretaría General de la Facultad.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
México, D.F., a 3 de noviembre de 1999.



DR. IVAN LAGUNES PEREZ
DIRECTOR DEL SEMINARIO DE DERECHO CIVIL.

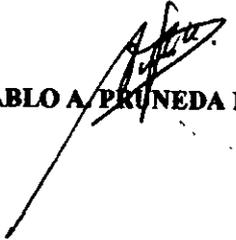
México, D.F., a 30 de septiembre de 1999.

DR. IVAN LAGUNES PEREZ.
DIRECTOR DEL SEMINARIO DE DERECHO CIVIL
FACULTAD DE DERECHO

Por medio de la presente deseo hacer de su conocimiento que en la tesis de la alumna DURÁN MORA MÓNICA con número de cuenta 9450970-4 titulada "EL DOCUMENTO ELECTRÓNICO COMO FORMA DE CONTRATACIÓN" encomendada a mi asesoramiento se ha concluido satisfactoriamente con la investigación, y otorgo mi voto aprobatorio a la misma, por lo que se somete a su apreciable consideración.

Sin más por el momento, de antemano agradezco su atención.

ATENTAMENTE.


LIC. PABLO A. PRUNEDA PADILLA

Como manifestación pura de la conciencia del Creador, mi obra es su obra y sólo existo por su infinita verdad. Y así surgi con un caudal inagotable de energía que fluía de forma caótica, al mismo tiempo que creaba destruía; camine caminos insospechados y descubrí lo desconocido, y aún así la duda y la indecisión me asediaban, entonces mis progenitores se convirtieron en mis guías, me acompañaron, enseñaron, amaron, cuidaron y protegieron para que pudiera descubrir quién soy, y por qué soy; y por eso les agradeceré eternamente y les dedico esta tesis a mis padres.

En palabras de Albert Einstein "el arte supremo del maestro es despertar el gozo por la expresión creativa y el conocimiento", y yo les agradezco a todos mis maestros por ello, pero con especial afecto al Lic. Pablo A. Pruneda Padilla quien sabiamente asesoró esta tesis, y al Dr. Iván Lagunes Pérez quien con sus correcciones la enriqueció.

Por sus conocimientos y apoyo incondicional agradezco a mi hermano.

Por su sabiduría y auxilio agradezco a familiares y amigos, así como a todos aquellos que hayan colaborado en la elaboración de la presente tesis.

EL DOCUMENTO ELECTRÓNICO
COMO FORMA DE CONTRATACIÓN

INTRODUCCIÓN

Nuestros tiempos se encuentran marcados con un constante avance tecnológico que ha llevado al ser humano a lograr metas antes insospechadas. El desarrollo tecnológico que inicio restringido a ciertas esferas de la actividad humana actualmente abarca la mayoría de nuestros actos, a este fenómeno se le ha denominado "Revolución Digital" y ha sido objeto de iniciativas de acción globales en Estados y en Europa; coincidiendo dichas iniciativas en que deben considerarse como fundamentales para lograr efectivamente el ingreso de la sociedad en la era informática: la información, la educación de los usuarios, la privacidad y la seguridad. Desgraciadamente, en nuestro país no se ha dado un movimiento de tanta trascendencia, pero ello, en diversas ocasiones nos servirá para apoyarnos en la experiencia adquirida por otras naciones, evitando cometer los mismo errores.

La informática ha llegado al campo del Derecho, es común para los juristas el uso de computadoras y programas en su labor diaria; asimismo, la implementación de tecnología día a día es más común para todos los seres humanos y es cotidianamente usada en sus relaciones, situación que acarrea como consecuencia la necesidad de que nuestro Derecho abarque los nuevos sistemas de contratación. Este fenómeno afecta la conducta del hombre, por lo que debe ser regulado a fin de evitar su aplicación indiscriminada y tutelar la seguridad y confianza de los contratantes ante la contratación electrónica.

Hoy en día las computadoras representan el mejor medio para satisfacer necesidades sociales, lo que nos ha llevado a que gran parte de la actividad documental se desarrolle en forma automatizada, con lo que llega la creciente tendencia de sustituir el documento escrito de manera tradicional y firmado a puño y letra, por el documento electrónico y la firma digital. La tecnología ha creado un nuevo reto que debe ser investigado y estudiado por el Derecho. El estudio de este fenómeno deberá abarcar el mayor campo posible, pero debe realizarse un especial esfuerzo en el ámbito jurídico afectado por el Internet, al ser una red abierta reconocida en nuestros días como la autopista de la información de más fácil acceso para el público en general, y cuya difusión, en opinión de la doctrina puede acarrear las mayores dificultades, debido a su constante uso y a la falta de conocimiento de la población en general de la importancia y características de la nueva era digital y sus aplicaciones.

CAPÍTULO

I

LA REVOLUCIÓN DIGITAL.

La informática es considerada como un fenómeno social al haber plasmado una diferencia en la vida humana, y ser un elemento determinante en el desarrollo del hombre.

La creciente necesidad de información y la velocidad con que la informática se extiende e incorpora a las actividades humanas ha calificado a este fenómeno de revolucionario; siendo considerado tan importante como el arte de labrar la piedra (época neolítica), el descubrimiento de la imprenta y la invención de la máquina de vapor que originó la Revolución industrial. Todos ellos fenómenos que en su momento transformaron al mundo.

La informática no debe ser menospreciada como el instrumento al servicio del hombre que lo ha liberado de la realización de las más pesadas cargas intelectuales, pero nunca podrá llegar a sustituir al ser humano; asimismo, se encuentra al servicio del Derecho, pero éste no debe someterse a ella.

La llamada "Revolución Digital" o "Revolución Informática" se encuentra en desarrollo constante, constituye parte de nuestra realidad e implica al Derecho, siendo esencial que nos preparemos para ella en vez de limitarnos a sufrir las repercusiones que dicho fenómeno traiga consigo.

1.1. La cibernética.

El término "cibernética" proviene del griego *kybernetes*, que significa, arte del piloto o timonel, y de *kybernes*, arte de gobernar, por lo que no es de extrañarse que dicha palabra haya sido utilizada tanto para abarcar estudios de ciencia política como de carácter matemático.¹

Derivado de lo anterior, en un principio el vocablo "cibernética" fue utilizado en 1848 por el francés Ampere para manifestar el arte del gobierno en sentido político. Pero fue hasta años después cuando la cibernética cobró especial relevancia.

En 1940, la cibernética comenzó a tener un nuevo significado cuando Norbert Wiener con la colaboración de otros científicos inició ciertos estudios estadísticos para aplicarlos durante la Segunda Guerra Mundial; éstos estudios fueron el primer paso para que Wiener

¹ "Enciclopedia Salvat". Tomo 2. Salvat editores, España, 1976, pág. 1156.

elaborara la teoría de la retroacción o *feed-back*, fundamentada en el uso de la retroalimentación de la información y de la relación hombre-máquina.

Sin embargo, no se deben desestimar los esfuerzos realizados por un fisiólogo mexicano de nombre Arturo Rosenblueth, ya que con su artículo analítico sobre el futuro desarrollo de la cibernética (publicado en 1943) se sentaron las bases para que en 1949 el científico Norbert Wiener publicará su libro "Cibernética o control y comunicación en el animal y en la máquina", en el cual el término "cibernética" fue empleado para denominar a una nueva ciencia² que trata de la comunicación y control entre las máquinas y el hombre.

Como el título de su libro lo indica, Wiener basado en un criterio matemático-fisiológico intentó establecer los fundamentos de la cibernética como ciencia que se ocupa de cualquier sistema, ya sea animal o artificial, obteniendo una ciencia que abarca de manera total e interdisciplinariamente a las demás.

A partir de ese momento se introdujeron los conceptos de "retroalimentación" y "sistema" originando la revolución del pensamiento científico hacia la consideración de que la realidad es una totalidad o continuo interactuante y regulable de hechos. Dentro de los factores que determinaron el surgimiento de la cibernética encontramos que se necesitaba una nueva disciplina que contribuyera al incremento de la producción, y por lo tanto del capital; además de que nació la necesidad de la aparición de una nueva disciplina que controlará y logrará una unidad multidisciplinaria con todas las ciencias.

Desde su creación numerosas definiciones se han aplicado a la cibernética, entre ellas encontramos las de los siguientes autores:

- ◆ La cibernética abarca la función del cerebro con respecto a las máquinas. Joan Corominas.³
- ◆ La cibernética es el estudio de sistemas abiertos en cuanto a la energía y cerrados en cuanto a la información y al control. W. Ross Ashby.⁴
- ◆ La cibernética es el estudio analítico del isomorfismo de la estructura de las comunicaciones en los mecanismos, en los organismos y en las sociedades, entendiéndose por isomorfismo una identidad entre dos sistemas, -donde las partes del sistema tienen relación entre ellas sin alterar el todo- que para que exista se requiere de determinadas relaciones entre los objetos del otro. N. Wiener.⁵
- ◆ La cibernética es la "teoría de los sistemas de control basada en la comunicación (transferencia de información) entre sistema y medio circundante, y dentro del sistema, y en el control (retroalimentación) del funcionamiento del sistema en consideración al medio". Ludwig von Bertalanffy.⁶

² La ciencia es comúnmente definida como el conocimiento cierto de las cosas por sus principios y sus causas; siendo la tecnología la aplicación de esos conocimientos.

³ Citado por Téllez Valdés, Julio. "Derecho Informático". McGraw-Hill, México, 1997, pág. 4.

⁴ Citado por Ríos Estavillo, Juan José. "Derecho e Informática en México". UNAM, México, 1997, pág. 37.

⁵ Idem.

⁶ Citado por Fix Fierro, Héctor "Informática y Documentación Jurídica". UNAM, México, 1990, pág. 42.

Un análisis de las definiciones anteriores nos indica como constantes al control, a la comunicación⁷ y al sistema, por lo que la cibernética es “una rama de la ciencia que estudia los procesos de comunicación y de control automáticos en los sistemas, bien sea que se trate de conjuntos o de individuos formados por máquinas, organismos biológicos o sistemas sociales”.⁸ Aunque puede irse más allá y definirse en los términos de K. Schnedier: “la cibernética no constituye un sistema acabado y autónomo, sino que representa el fundamento teórico de cualquier sistema susceptible de asumir un carácter cibernético. El método para la elaboración del modelo cibernético se basa en la reducción a un principio fundamental de carácter formal y abstracto de todas las posibilidades dinámicas de un sistema”.⁹

En cuanto a la cibernética relacionada con las disciplinas sociales, resulta necesario precisar que la cibernética se encuentra íntimamente ligada con la teoría general de los sistemas; en dicha forma de pensamiento se trata con “totalidades” en todos los campos del conocimiento, por lo cual la cibernética y la teoría general de los sistemas han recibido fuertes críticas, ya que si bien han tratado de actuar como puente entre las ciencias y como punto de conexión entre los mundos tecnológico y humano, también han tratado de fungir como un esquema general aplicable a cualquier campo del conocimiento; han tratado de hacer extensivos sus conceptos a otras disciplinas, buscando más el control de los fenómenos que su explicación causal. Siendo lo cierto que “la aplicación de estas teorías a los fenómenos sociales encuentra sus límites en las cuestiones valorativas, que no pueden resolverse siguiendo simples criterios de regulación y de control”.¹⁰

Por su parte, el autor Norbert Wiener también escribió una obra denominada “The Human Use of Human Beings” (traducido al español como “Cibernética y Sociedad”) en la que plasma que los problemas de la Ley deben ser considerados como problemas de control ordenado; por lo que la mayor relación entre cibernética y Derecho se encontrará en las áreas donde exista mayor precisión en los conceptos y estrictas reglas formales, pero como es lógico de suponer ni en aquellos días ni en nuestros tiempos se ha logrado, ni se logrará reducir al Derecho a un sistema de axiomas, prevaleciendo la opinión de que tanto la cibernética como la informática sólo pueden actuar, en este caso, como instrumentos al servicio del Derecho, y por otro, como los representantes de una nueva civilización cuyas consecuencias deben ser jurídicamente reguladas.

⁷ La comunicación es proceso esencial en la sociedad, y es definida por el autor Juan José Estavillo como la exteriorización del pensamiento del hombre dentro de su esfera personal, mediante un proceso de transmisión, a través de un canal a otra persona con el fin de ejercer en esta última cierta interacción o producir en él algún estímulo. En términos generales el proceso de la comunicación se encuentra representado por un emisor, un transmisor o canal que lleva implícito el mensaje, y por un receptor. Ríos Estavillo, Juan José. Ob. cit., p.p. 9 y 10.

⁸ Padilla Segura, José Antonio. “Informática Jurídica”. SITESA, México, 1991, pág. 54.

⁹ Citado por Ríos Estavillo, Juan José. Ob. cit., pág. 55.

¹⁰ Zippelius citado por Fix Fierro, Héctor. Ob. cit., pág. 43.

1.2. Las computadoras.

En un comienzo la utilización de la computadora se vio restringida, y su futuro era incierto. Las primeras computadoras eran lentas y de gran tamaño por lo que se dudaba de su utilidad práctica, pero con el paso del tiempo los ordenadores disminuyeron en tamaño y aumentaron en velocidad, con lo que se inició su producción a gran escala, hasta llegar en nuestros días a tener un uso casi universal. Sin embargo, en nuestro país el uso de la computadora se ha visto limitado, principalmente porque el acceso a ellas¹¹ depende del nivel de ingresos de la población.

1.2.1. Historia y desarrollo.

Por lo general, el desarrollo de las computadoras se ha dividido en generaciones, a saber:

Primera generación (1944-1951). Las computadoras pertenecientes a esta generación se caracterizaron por ser de gran tamaño y peso, eran lentas, se sobrecalentaban con facilidad, poseían capacidad de almacenamiento interno muy limitado, usaban circuitos de tubos al vacío o bulbos como componentes básicos de sus circuitos internos, y el lenguaje para su programación era el binario. A esta generación pertenece el origen de las computadoras, el cual se desarrolló de la siguiente manera:

En el siglo XVII las primeras máquinas procesadoras de datos se usaron para realizar cálculos numéricos de manera mecánica utilizando ruedas, piñones, engranes y palancas.

En 1642 Blas Pascal ideó la primera máquina para calcular, pero fue en 1890 cuando en el censo de Estados Unidos se dio el gran paso hacia la era de la computación.

En Francia, en 1804 Joseph Marie Jacquard, construyó una máquina para tejer diversos diseños de telas, dicha máquina introdujo la automatización y el uso de tarjetas perforadas en las que se almacenó la información del camino que debían seguir los hilos de la tela para crear el diseño escogido.

Entre 1791 y 1871, el inglés Charles Babbage diseñó diversos proyectos entre los que se encontró una máquina capaz de realizar cálculos complejos y una máquina analítica caracterizada por poseer una parte que ordenaba y otra que ejecutaba las órdenes; y a pesar de que ninguna se puso en funcionamiento, su máquina analítica es considerada como la que sentó las bases para la primera computadora electrónica.

El sistema de tarjetas perforadas fue implementado en 1880 por el estadista Herman Hollerith, que trabajaba en la Oficina de Censo de los Estados Unidos; él usó un sistema que representaba por medio de agujeros en una tarjeta los datos esenciales de cada persona, para después contarlos electrónicamente.

¹¹ Incluyendo el acceso a diversas herramientas tecnológicas como el Internet.

La velocidad para la obtención de información demostrada por las máquinas de Hollerith provocaron su uso en diversos países, razón por la cual, posteriormente fueron perfeccionadas y utilizadas para la realización de diversas operaciones que implicaban la solución de problemas contables y administrativos. En 1986 Hollerith organizó la Compañía de Máquinas Tabuladoras, la que continuó desarrollando las máquinas y las comercializó.

Entre 1900 y 1940 las máquinas electromecánicas son perfeccionadas y encuentran cada vez mayor aplicación en el comercio y en la industria.

En 1943 John von Neumann, miembro de la Universidad de Princeton, trajo al mundo la concepción de una computadora con capacidad para almacenar programas.

En 1944, Howard Aiken, en la Universidad de Harvard, con el apoyo de IBM, desarrolló y puso en funcionamiento a la primera computadora electromecánica automática de uso general; a dicha máquina se le denominó Mark I o ACSS (Automatic Sequence Controlled Calculator). Siguiendo sus pasos en 1946 surgió la primera máquina calculadora completamente electrónica concebida por un equipo dirigido por los ingenieros John Mauchly y John Eckert de la Universidad de Pennsylvania, a la que se dio el nombre de ENIAC (Electronic Numerical Integrator and Computer). Esta máquina se utilizó de forma primordial para resolver problemas de balística y aeronáutica; funcionaba a base de 18 000 bulbos y ocupaba una superficie de 180 metros cuadrados.

En 1949, Mauchly y Eckert, en la Universidad de Cambridge, Inglaterra, crean a la computadora denominada EDVAC (Electronic Discret Variable Automatic Computer), con capacidad para almacenar programas. A esta máquina se le reconoce como el prototipo de los actuales procesadores electrónicos.

Iniciándose en 1951 la producción comercial de computadoras basado en un modelo de computadora digital electrónica denominado UNIVAC I (Universal Automatic Computer); computadora de uso comercial, desarrollada por la Compañía Remington Rand fundada por los creadores de EDVAC. Dentro de las innovaciones aplicadas a esta computadora se encuentran el uso de cinta magnética para la entrada y salida de datos, y el uso de un programa especial que traducía programas de un lenguaje particular al de la máquina.

Segunda generación (1951-1963). El tamaño de las computadoras se reduce y aumenta su capacidad de procesamiento. Están construidas por circuitos transistores y se programan con lenguajes "de alto nivel". A partir de esta generación surgen tecnologías complementarias de las computadoras como las memorias auxiliares (discos y cintas), impresoras, etcétera.

Tercera generación (1963-1971). Los lenguajes de control se constituyen como sistemas operativos y se usan circuitos integrados monolíticos con lo que aumenta su confiabilidad, y se reduce el costo y el tamaño. A partir de este momento se da un desarrollo constante en el área computacional, encontrándose esta industria en segundo

lugar después de la automotriz. Siendo un año importante 1965, fecha en la que se registra la instalación de la primera minicomputadora comercial.

Cuarta generación (1972-1982). Se da la integración a larga escala (LSI), y microcircuitos integrados en placas de silicio denominados chips. Surgen los microprocesadores, circuitos integrados de alta densidad, y traen consigo a las computadoras personales. Se utiliza de forma continua el proceso de miniaturización de los circuitos y aumenta la velocidad y la capacidad de las computadoras. Las computadoras de la cuarta generación son las que de forma general se utilizan en nuestros días.

Quinta generación (1983-). Dada la competencia por desarrollar tanto las computadoras como los sistemas y el software necesarios para su funcionamiento dentro de esta generación se encuentran equipos de proyección a futuro que darán prioridad a las funciones lógicas. Dentro de los principales objetivos a desarrollar se encuentran: el lograr que la computadora maneje el lenguaje natural en vez de códigos especializados; crear circuitos de gran velocidad, así como sistemas de inteligencia artificial; y obtener el procesamiento en paralelo mediante arquitecturas y diseños especiales. Asimismo, se espera que continúe el proceso de miniaturización, una baja en los costos de fabricación, una creciente integración de la informática y las telecomunicaciones, y la aplicación de los ordenadores a nuevas áreas y actividades, previéndose un auge en el correo, las compras y el banco electrónico, así como en los sistemas de aprendizaje vía computadora.

1.2.2. Concepto.

La computadora se puede definir como una "calculadora electrónica universal que, beneficiándose del control de un detallado programa registrado en sus órganos de memoria, efectúa automáticamente conjuntos complejos de operaciones aritméticas y lógicas".¹²

Hoy en día las computadoras son instrumentos comúnmente utilizados por el hombre, se usan tanto en las más grandes organizaciones como en los hogares, logrando junto con otras tecnologías de la información un impacto social, político, económico y cultural, que se ha traducido en el surgimiento del fenómeno llamado "civilización tecnológica"; pero su desarrollo ha continuado hasta abarcar niveles antes considerados únicamente como humanos, como es el caso de la inteligencia, ante lo que se ha generado temor y desconcierto por su uso.

En vista de lo antes mencionado aún no se ha logrado determinar si la repercusión de las computadoras en la vida del hombre ha tenido más efectos positivos que negativos, pero sí se reconoce a la tecnología como una condición del poder y por lo tanto de control social, por lo que el grado de afectación que actualmente estamos viviendo es sólo el comienzo de lo que llegará a ser. Para el autor Julio Téllez Valdés¹³ dentro de las implicaciones positivas y negativas del uso de las computadores se pueden señalar:

¹² Gran Diccionario de las Ciencias. Tomo IV. Larousse, España, 1987, pág. 787.

¹³ Téllez Valdes, Julio. Ob. cit., pág. 23.

Implicaciones positivas:

- ◆ Nuevas oportunidades de trabajo. En nuevas áreas como la programación, operación y mantenimiento de computadoras y administración de sistemas de información.
- ◆ Mayor satisfacción en el trabajo. Las computadoras contribuyen a resolver problemas más complejos, ellas realizan las tareas repetitivas y aburridas dejando al ser humano concentrarse en aspectos más trascendentes.
- ◆ Aumento en la productividad. Evitan el desperdicio y mejoran la eficiencia, e incluso auxilian para dar un mejor servicio a los clientes.

Implicaciones negativas:

- ◆ Amenaza de desempleo. Por el reemplazo del trabajador humano por la máquina.
- ◆ Alta dependencia de la tecnología. Al respecto el autor García Pelayo considera que la tecnología “parece haber creado una nueva naturaleza (artificial), un medio ambiente que parece seguir sus propias leyes y del que el hombre es tan poco dueño como lo puede ser ahora del clima. De ahí los llamados efectos de “gran tecnología”: la sociedad se vuelve dependiente de la tecnología y, por lo tanto, altamente vulnerable”.¹⁴
- ◆ Problemas físicos y psicológicos. Como la despersonalización, trastornos visuales, etcétera.
- ◆ Problemas jurídicos. Ante la necesidad de un marco de regulación.

Sin embargo se debe precisar que las computadoras, como cualquier herramienta tecnológica creada por el hombre, en sí mismas no acarrear implicaciones positivas o negativas. Es el hombre quien especifica el funcionamiento de las herramientas que construye, siendo el elemento humano el que determina las consecuencias de su aplicación.

1.3. La informática.

La creciente necesidad de información clara, inteligible, relevante, completa, oportuna y confiable, nos lleva a tener que considerar a la misma como fundamental para el desarrollo de las actividades humanas y como transformadora y reorganizadora de nuestra sociedad y nuestra economía.

La información¹⁵ inteligente o *know-how* con posibilidades de aplicación trasciende las fronteras geográficas del lugar donde se originó y se produce en cantidades antes insospechadas, por lo que no puede menos que considerársele una de las mercancías más solicitadas e incluso una materia prima inagotable de la acción social; siendo la informática la que permite tener acceso a todos los conocimientos de la humanidad de manera rápida y efectiva.

¹⁴ Citado por Fix Fierro, Héctor. Ob. cit., pág. 48.

¹⁵ Para López Ayllón la información es “un conjunto de mecanismos que permiten al individuo reformar y organizar los datos del medio para que, estructurados de una manera determinada, le sirvan de guía de acción”. Ibidem, pág. 61.

El vocablo “informática” es un neologismo introducido en 1962 por Philippe Dreyfus y proviene de la unión de las palabras *information* y *automatique* tratando en un principio de implicar a la ciencia del tratamiento automatizado de la información, esencialmente a través de la utilización de las computadoras. Sin embargo, desde hace décadas, la informática comenzó a extenderse a casi todas las áreas del que hacer humano dificultando la creación de una definición integral.

Para definir a la informática se han tomado en cuenta diferentes aspectos generales dentro de los que se encuentra el hecho de que no se le puede confundir con el simple uso de una computadora, ya que es una disciplina con fines específicos que implica el tratamiento automatizado de la información. En base a lo anterior a la informática se le ha considerado como “el estudio que delimita las relaciones entre los medios (equipo), los datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado”¹⁶ o como el “producto de la cibernética, en tanto un proceso científico relacionado con el tratamiento automatizado de la información en un plano interdisciplinario”.¹⁷

La informática considerada como la parte de la cibernética relativa al tratamiento automatizado de la información en un plan operativo e interdisciplinario, ha sido definida por el Doctor Enzo Molino del CONACYT como¹⁸:

- ◆ Ciencia que se ocupa del proceso y almacenamiento de información mediante computadoras.
- ◆ Ciencia que tiene que ver el procesamiento de información, particularmente con el que utiliza medios y dispositivos automáticos.
- ◆ Ciencia que estudia los métodos y medios necesarios para el tratamiento sistemático y eficaz de la información.

Siendo una definición completa la que nos da el autor José Antonio Padilla Segura¹⁹, al ser él quien profundiza en el estudio del tema, indicando que la informática es el conjunto de disciplinas y técnicas para la elección, captación, almacenamiento, procesamiento, organización y recuperación de datos a fin de contar con una información eficiente y con una comunicación eficaz dentro de un sistema, sea político, social o económico, tratados en forma racional, generalmente empleando medios o recursos automatizados o de difusión; tales como son las computadoras y los sistemas modernos de telecomunicación, para aplicarlos a la comprensión de situaciones y a la solución de problemas. Sin embargo, el propio autor manifiesta que dicha definición es incompleta; porque la informática va más allá de ser una disciplina científica o técnica, ya que ha penetrado en todos los campos del saber y del que hacer humanos.

¹⁶ Mora, José Luis y Molino, Enzo citados por Téllez Valdés, Julio. Ob. cit., pág. 5.

¹⁷ Losano, Mario G. citado por Téllez Valdés, Julio. Idem.

¹⁸ Citado por Padilla Segura, José Antonio. Ob. cit., pág. 55.

¹⁹ Ibidem, pág. 5.

Asimismo, es necesario precisar que si bien la informática, es un apoyo para el desarrollo de cibernética, también es una ciencia particular integrada a la cibernética; ambas tratan la información de manera matemática, pero entre ellas existen diferencias de objeto y finalidad que deben resaltarse: La cibernética abarca el control y la comunicación, mientras que la informática se restringe al tratamiento automático y representación de la información. Así, la informática comprende la programación, estructura de la información, ingeniería del software y hardware, entre otras materias; mientras que la cibernética entre otros aspectos, abarca la creación de instrumentos informáticos que simulen actividades del hombre, como es el caso del desarrollo de la inteligencia artificial.

1.3.1. La teleinformática.

La teleinformática o telemática es una rama de la informática que comienza a tener importancia en los años sesenta pero alcanza su auge hasta los setenta, siendo su principal característica el uso conjunto de las telecomunicaciones y de la informática con el propósito de transmitir información procesada a distancia. Actualmente los satélites artificiales -en especial los de comunicación geoestacionarios-, así como las microondas y las fibras ópticas, le han brindado a la informática la posibilidad de tener una cobertura universal.

Gracias a la teleinformática se ha extendido el uso de las computadoras para que un sinnúmero de personas pueden acceder a potentes ordenadores situados a distancias considerables, así como a bancos de datos de programas que les permiten disponer rápidamente de la información necesaria.

1.4. Internet.

Internet también conocida como la Red (*the Net*), es la red de computadoras más grande del mundo; ella anticipa el futuro de las telecomunicaciones por lo que ha adquirido la categoría de precursora de la supercarretera de la información. "La Red se creó para ser autónoma, con la capacidad de transmitir comunicaciones rápidamente sin el control de persona o empresa comercial alguna".²⁰

Internet más que una red de trabajo, es la red de redes para el intercambio internacional de información con limitadas restricciones, no existiendo una institución que por sí misma pueda administrarla, ni un sólo lugar donde se centralice toda la información, ni en donde se registren todos los contactos. Es una herramienta al servicio del hombre que nos brinda información en calidad y cantidad que es difícil describir, es una herramienta flexible en la que se puede acceder tanto a información invaluable como a corrupción de menores. Internet es la herramienta que nos facilita la recolección de información para que posteriormente usando nuestro raciocinio la interpretemos y usemos a nuestra conveniencia.

²⁰ Barrios Garrido, Gabriela; et al. "INTERNET y Derecho en México". McGraw-Hill, México, 1997, pág. 10.

La Red es tan grande que nadie conoce con exactitud su tamaño; se calcula que en 1981 tan sólo existían 300 computadoras enlazadas, aumentado la cantidad de manera considerable para 1997, año en el que Internet ya abarcaba todos los continentes con aproximadamente 25000 redes conectadas y 40 millones de usuarios (de los que el 60% corresponden únicamente a Estados Unidos); existiendo de forma aproximada 200 millones de usuarios en el presente año. Internet crece alrededor de un 10 por ciento cada mes, por lo que diversos estudios calculan que en ocho años, quinientos millones de personas usaran la Red.²¹

Internet es una de las redes más abiertas del mundo al ser de acceso general, además de que actúa como su propia fuente de software y se ha convertido en uno de los medios más importantes para el desarrollo del comercio. La Red implica un obstáculo para el establecimiento o mantenimiento de barreras sociales, ya que se funda más en apariencias que en realidades, por lo que en ella interactúan desde importantes redes corporativas como AT&T y Hewlett-Packard hasta compañías pequeñas e informales, intercambiándose información que une desde personas hasta gobiernos, de manera casi instantánea.

En el comercio la Red ha incrementado la competencia, y ha proporcionado nuevas oportunidades de mercado; dependiendo mucho el desarrollo de los negocios en Internet del dinero electrónico (e-money) para los pagos.

Además de los beneficios antes mencionados podemos señalar que la Red permite establecer una conexión nacional o internacional al costo de una llamada local, reduce considerablemente el tiempo de transmisión de la información, y facilita el envío de mayor cantidad de datos, además de que gracias a los navegadores (browsers) Internet es una herramienta fácil de usar. Pero Internet también acarrea problemas, siendo de especial importancia, en cuanto a transacciones comerciales y suministro de información privada, los de confidencialidad y del monitoreo de acceso; aunque actualmente la propia tecnología brinda soluciones a estos problemas.

Internet es una de las manifestaciones de la revolución tecnológica que se desarrolla a cada momento e implica el inicio de una sociedad interconectada acorde con la globalización, acarreado la modificación de las prácticas tradicionales de diversas disciplinas del conocimiento, entre ella las del Derecho. Sin embargo, la Red comienza a sufrir estragos técnicos como el "congestionamiento" en horas pico y en lugares de gran interés, por lo que el uso de Internet también trae consigo retos tecnológicos.

Dentro de los servicios disponibles en Internet se encuentran:

- ♦ Correo electrónico (e-mail). Para utilizar este servicio es necesario poseer una dirección de correo electrónico. El e-mail es uno de los medios más usados para el intercambio de información, a través del envío y recepción de mensajes, funcionando

²¹ Ibidem, p.p. XVII y 5.

de forma parecida al servicio postal.²² Dentro este servicio se encuentran listas de correo y los servidores de correo:

- * Las listas de correo constituyen una lista de usuarios que desean intercambiar información sobre un tema específico, pero a diferencia del correo electrónico, la información se distribuye automáticamente a todos los suscriptores.
- * Siendo los servidores de correo programas que responden a mensajes de correo electrónico.
 - ◆ Conversaciones en línea (IRC: Internet Relay Chat). Es un servicio usado para “charlar” en tiempo real con otros usuarios cuyas computadoras se encuentren interconectadas en el momento de la sesión.
 - ◆ Software gratuito. La Red permite que se tenga acceso a diversos programas sin costo alguno.
 - ◆ Boletines electrónicos (BBS: Bulletin Board Systems). Lo utilizan desde usuarios particulares hasta compañías comerciales para difundir información específica.
 - ◆ Telnet. Permite a través de la interconexión y de forma interactiva el acceso remoto a sistemas, programas o aplicaciones disponibles en otro ordenador (por lo general, de gran capacidad). Su uso es ocasional y en muchas ocasiones se circunscribe a los casos de sistemas de información que operen sobre la base de sistemas de búsqueda específicos.
 - ◆ Protocolo de Transferencia de Archivos (FTP: File Transfer Protocol). Constituye una versión reducida de Telnet al únicamente usarse para transferir archivos.
 - ◆ Grupos de discusión o foros. Los foros no implican al correo electrónico y en ellos se intercambia información sobre un tema en particular. Sin embargo, la comunicación no se da en tiempo real ni directamente entre los participantes, ya que cada uno deja su punto de vista o aportación para que posteriormente otro miembro del grupo lo consulte.
 - ◆ World Wide Web (WWW o Web). Permite hacer una consulta y transmitir información gracias a los enlaces de hipertexto²³ insertados en el texto por el autor. Los servidores Gopher fueron los primeros intentos para integrar los recursos de la Red, pero actualmente están siendo sustituidos por el Web.

1.4.1. Antecedentes.

Internet se basó en ARPANET (donde ARPA corresponde a la agencia de Investigación de Proyectos Avanzados -Advanced Research Project Agency-), proyecto del Departamento de Defensa de Estados Unidos (DOD) creado en 1969 para enlazar a este Departamento con los encargados de efectuar investigaciones militares, siendo algunos de ellos laboratorios universitarios donde se realizaban investigaciones sobre defensa, asimismo, se trataba de obtener una red confiable que utilizara un cambio de ruta dinámico, a través del cual en caso del ataque enemigo, si uno de los enlaces de la red se interrumpiera, el tráfico en éste podría desviarse automáticamente hacia otros enlaces.

²² Con la diferencia de que en el caso del correo electrónico la información tarda de segundos a minutos en transmitirse.

²³ Manifestado con palabras subrayadas o resaltadas del texto.

ARPANET se extendió con rapidez por el deseo de todas las universidades de los Estados Unidos de afiliarse; el creciente número de usuarios conectados dificultó las funciones de ARPANET provocando que se dividiera en dos secciones: MILNET, que abarcaba los aspectos militares y ARPANET, que se ocupó de los servicios civiles. Sin embargo, las secciones permanecieron conectadas a través del protocolo de Internet (IP).

El IP fue diseñado para soportar miles de redes de trabajo, e introdujo la posibilidad de que las terminales se comunicarán entre sí, además de que se continuará dando la transmisión de información de las terminales hacia los sistemas centrales y viceversa.

El aumento de usuarios continuó su marcha e hizo evidente la ineficacia de ARPANET, por lo que en 1984 la Fundación Nacional de Ciencia (NSF: National Science Foundation) estableció cinco centros de cálculo equipados con supercomputadoras para permitir que los investigadores, a través de ARPANET, tuvieran acceso a la información almacenada, y pudieran enviar sus programas a la supercomputadora y recibir los resultados en el lugar de envío; sin embargo este proyecto no funcionó, por lo que la NSF creó su propia red para conectar sus cinco centros de supercomputadoras, dando origen a NSFNET.

A la NSFNET se conectaron todas las redes de trabajo regionales, a las que a su vez se conectaron los usuarios de cada zona; por lo que después de 20 años de servicios ARPANET fue cancelada en marzo de 1990, siendo sustituida por NSFNET.

Con el paso del tiempo las supercomputadoras se volvieron inefectivas pero NSFNET subsistió gracias a su fácil integración al medio Internet.

En un principio la NSFNET permitió únicamente el tráfico relacionado con la investigación y la educación, quedando los servicios IP independientes y los comerciales para las demás actividades, sin embargo, en 1987 la NFS realizó un contrato con Merit Network Inc., IBM y NCL para administrar efectivamente e incrementar la capacidad de la red, pero en 1992 la NFS retiró su inversión y con ella su influencia netamente científica, para dar paso al uso comercial de la red, así como a su creciente desarrollo en años recientes.

En febrero de 1989 México fue el primer país latinoamericano en conectarse a Internet. La conexión se realizó a través de Teléfonos de México, y al igual que en Estados Unidos en un inicio la Red se usó con fines de educación e investigación en el Instituto Tecnológico de Estudios Superiores de Monterrey, el Instituto Politécnico Nacional, la Universidad Nacional Autónoma de México, la Universidad de Guadalajara y la Universidad de las Américas (Puebla), hasta que en 1994, comenzó la participación de empresas privadas y con ellas la utilización comercial de Internet.

En años recientes la demanda de Internet en México se ha incrementado; durante 1994 y 1995 surgieron diversas compañías dedicadas a vender el acceso a la Red, al diseño y colocación de páginas en el WWW, y a la venta de contenidos informáticos. Existiendo 158 servidores en 1996.²⁴

²⁴ Barrios Garrido, Gabriela. Ob. cit., pág. 11.

En nuestro país, a pesar de que en muchos aspectos apenas se está reconociendo la utilidad de Internet, su desarrollo la ha llevado a ser de interés general, abarcando tanto al sector público como al privado, por lo que el Instituto Nacional de Estadística, Geografía e Informática (INEGI), la Presidencia de la República, y la Procuraduría General de la República, entre otras, han tratado de generalizar el uso de la Red y se encuentran analizando la aplicación de ésta herramienta en el sector gubernamental (por ejemplo, para la prevención e investigación del delito). Por desgracia, en algunos sectores aún se carece de datos actualizados, así como de la infraestructura necesaria para un eficaz funcionamiento.

1.4.2. Funcionamiento.

La Red en general funciona como cualquier red de computación, donde cada mensaje específico es enviado a una computadora en particular, permitiendo que la computadora que recibe un mensaje pueda a su vez enviar una respuesta a la que se lo envió.

Internet enlaza una multitud de redes dentro de las que se encuentran: redes de área local (LAN: Local Area Network), redes de área metropolitana (MAN: Metropolitan Area Network), y redes de área amplia (WAN: Wide Area Network).

En Internet, de forma técnica, a las computadoras conectadas directamente se les denomina anfitriones y a las computadoras conectadas a ellas se les llama usuarios.

Internet, se compone de una infraestructura compartida, constituida por todas las partes que manejen los protocolos preestablecidos,²⁵ y fundamentalmente, transmite información de una computadora a otra, para lo cual, en el caso de que la información se transmita del anfitrión A al anfitrión B, el anfitrión A se conecta a la red a la que se enlaza el anfitrión B de manera directa (o se deben lograr conexiones con diversas redes o incluso con varios anfitriones antes de que llegue la información a su destino final). Y en el caso del usuario, el funcionamiento es un poco más complicado. El usuario debe pagar una suscripción a un proveedor de acceso a Internet (ISP's: Internet Service Providers) conectado a la Red para que éste le proporcione el acceso a su red que a su vez se conecta a alguna de las redes que forman a Internet.

La conexión al proveedor de acceso puede darse por línea telefónica; mediante una conexión X.25, que ofrece mayor seguridad; o por líneas telefónicas arrendadas.

Por lo anterior, el funcionamiento de Internet es más parecido al funcionamiento del servicio postal que al teléfono; ello debido a que la comunicación vía telefónica se efectúa a través de un circuito eléctrico que conecta el teléfono del emisor con el del receptor por medio de una compañía que preste este servicio; pero en el caso del servicio postal el emisor envía la información en un paquete que entrega a la oficina de correos local, la cual a su vez es enviada a una oficina central, donde se clasifica por direcciones para enviarla a

²⁵ Un protocolo se constituye con reglas aceptadas para transmitir y recibir información.

otra oficina local y que ella entregue la correspondencia al receptor a través de un cartero. Asimismo, en Internet la información se transmite en paquetes.

En la Red se envían los datos en fragmentos en los denominados "paquetes", los cuales contienen la identificación del emisor y del receptor. Aunque a diferencia de la oficina de correos la información en Internet se transmite en segundos.

Internet es un conjunto de redes que envían y reciben paquetes entre sí utilizando el Protocolo Internet (IP). Diversos protocolos se usan en conexiones con IP, el cual posee un porcentaje de confiabilidad del 99%, siendo los más conocidos: el Protocolo para Control de Transporte (TCP), el Protocolo para el Datagrama del Usuario, y los protocolos creados por la Organización Internacional de Estandarización (ISO).

Protocolo para Control del Transporte. El Protocolo para Control de Transporte (TCP), al ser combinado con el IP es denominado TCP/IP, siendo éste el usado en la mayoría de las aplicaciones en la Red.

El TCP/IP es el que proporciona una conexión tan eficiente que a simple vista el funcionamiento de Internet puede confundirse con el del teléfono; el TCP/IP nos da la apariencia de que cuando una computadora se comunica con otra a través de la Red se crea un circuito físico, cuando en realidad lo que surge es un circuito virtual, formado por un conjunto de paquetes IP.

El TCP/IP asegura que los datos enviados lleguen efectivamente y de la manera en que fueron enviados al receptor. En ocasiones se pierde la información pero, por lo general, si no llega a su destino es reenrutada a la dirección del emisor.

Protocolo para el Datagrama del Usuario (UDP). Este protocolo es menos confiable que el anterior, aunque resulta efectivo para aquellas aplicaciones que poseen sus propias reglas sobre confiabilidad.

Protocolos creados por la Organización Internacional de Estandarización (ISO). Para asegurar la confiabilidad la Organización Internacional de Estandarización ha desarrollado un conjunto de protocolos de comunicación para remplazar a TCP/IP, sin embargo, la mayoría de éstos son complejos y lentos, por lo que casi se encuentran en desuso. Uno de los protocolos definidos por ISO es el X.25, el cual verifica paso a paso la transmisión de cada paquete, siendo hasta el momento el protocolo más confiable el denominado X.75.

1.4.2.1. Sistema de Nombre de Dominio.

En la Red cada anfitrión se identifica con un número y un nombre. Por lo general, las computadoras manejan los números binarios de 32 bits, pero al resultar esos números difíciles de memorizar, el número de anfitrión se dividen en cuatro partes, de ocho bits y cada parte se traduce en un equivalente decimal, por ejemplo, xxx.xxx.xx.x²⁶

²⁶ Donde cada "x" corresponde a un número entre el 0 y el 9.

Algunos anfitriones pueden tener más de un número o de un nombre debido a que se encuentran conectados a diversas redes, pero para localizarlos es indiferente cual de ellos se utilice.

En cuanto a los nombres, en un principio cuando funcionaba ARPANET cada máquina poseía un nombre de una fracción, sin embargo con el creciente incremento de computadoras distinguir las a cada una por nombre se hizo imposible, por lo que se recurrió al Sistema de Nombre de Dominio (DNS: Domain Name System) donde los nombres de los anfitriones son una serie de letras divididas en fracciones separadas por medio de puntos, por ejemplo, **calal.pull.com**, siendo indiferente el uso de mayúsculas o de minúsculas.

En Internet, por lo general, los nombres se codifican de derecha a izquierda, denominándose “zona” al extremo de más a la derecha, en nuestro ejemplo: **com**, de donde se infiere que se trata de un sitio comercial.

Las zonas se dividen en dos categorías generales, a saber, las de dos y tres letras. Las de tres hacen referencia al tipo de organización, es decir:

- com** Organizaciones comerciales.
- edu** Instituciones educativas.
- gov** Cuerpos y departamentos gubernamentales.
- int** Organizaciones internacionales.
- mil** Emplazamientos militares.
- net** Organizaciones de manejo de redes.
- org** Organizaciones no lucrativas abarcando, por lo general, a las que no entran en ninguna de las categorías anteriores.

En cuanto a este tipo de zonas debe hacerse mención a que en el Memorándum de Entendimiento, emanado de la conferencia organizada por la Unión Internacional de Telecomunicaciones para reestructurar la forma de registro de los nombres de dominio con sede en Ginebra (del 29 de abril al 1º de mayo de 1997), se previó la creación de siete nuevos dominios, algunos de los cuales incluyen más de tres letras:

- firm** Empresas.
- store** Comercios.
- web** Organizaciones dedicadas a actividades que tengan relación con el WWW.
- arts** Actividades culturales y ocio.
- rec** Organizaciones relacionadas con actividades recreativas.
- nom** Sitios individuales Web.
- info** Servicios informativos.

Por su parte las zonas de dos letras corresponden a sitios geográficos, por ejemplo:

- AU** Australia.
- CA** Canadá.
- IT** Italia.
- JP** Japón.
- ES** España.

US Estados Unidos de América.

MX México.

La siguiente fracción del dominio, en nuestro ejemplo: **pull**, corresponde al nombre de la compañía, siendo la última fracción, para nosotros: **calal**, el nombre particular de cada máquina.

En México, la institución encargada de la asignación de nombres de dominio bajo **.mx** es el Centro de Información de Red de México (NIC: Net Information Center -México-), situado en el Instituto Tecnológico de Estudios Superiores de Monterrey, Campus Monterrey. Este Centro surgió en diciembre de 1995 y se encarga de la coordinación y administración de los recursos Internet asignados a México.

CAPÍTULO

II

LA INFORMÁTICA Y EL DERECHO.

La presencia de la informática, y de su más notoria herramienta, la computadora, se ha extendido hasta abarcar casi todas las áreas del conocimiento, incluyendo al campo de las humanidades.

De la influencia de la informática en el Derecho se han derivado dos líneas de investigación, a saber: la informática jurídica, que abarca la aplicación de la informática en el tratamiento de la información jurídica; y el Derecho de la informática, que comprende los aspectos normativos del uso de la informática. Siendo el Derecho Informático,¹ aquél que se ocupa del conocimiento de ambas líneas de investigación.

La doctrina considera que el Derecho de la informática y la informática jurídica encuentran un punto de intersección en cuanto a la reglamentación del uso y explotación de los sistemas de información jurídica.

2.1. Informática jurídica o jurismática.

La razón del surgimiento de la informática jurídica, se encuentra en un estudio clásico del autor Spiros Simitis publicado originalmente en 1970; en ese estudio se hacía mención a un fenómeno al que se denominó "crisis de la información jurídica".² Con ese término se trató de abarcar el hecho de que en ningún campo en el que se requiriera el conocimiento de las normas y procedimientos del Derecho escapaba a las crecientes dificultades de obtener información relevante.³

Ante la crisis de la información jurídica surgieron diversas soluciones, las cuales se clasificaron en dos grandes rubros: las soluciones "no tecnológicas" y las soluciones "tecnológicas". Las soluciones "no tecnológicas" se centraron en disminuir la cantidad de

¹ El Derecho Informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (Derecho de la informática). Téllez Valdés, Julio. Ob. cit., pág. 22.

² El término "crisis de la información jurídica" no se considera apropiado, ya que dicha denominación no hace sólo referencia al problema de acopio documental, sino que también implica la existencia de una crisis de la información jurídica en sí. Ríos Estavillo, Juan José. Ob. cit., pág. 28.

³ La información jurídica es aquella que se conforma de la determinación de las fuentes formales del Derecho. Es aquella que emana de uno o varios órganos del Estado, bajo un procedimiento determinado también en la ley, que darán contenido a las relaciones sociales bajo los principios y valores del Derecho como son el de bien común, la seguridad jurídica, y los principios generales del Derecho, entre otros. Ríos Estavillo, Juan José. Ob. cit., pág. 26.

información producida, por lo que no fueron efectivas. Así, las soluciones “tecnológicas” fueron las que resultaron realmente aplicables, consistiendo éstas en el uso de la computadora para el tratamiento de la información; surgiendo así la informática jurídica.

Nuestro país al igual que cualquier otro en el mundo no resultó exento de cruzar por la crisis de la información jurídica. En México la cantidad de información que emana tan sólo del Poder Legislativo y del Poder Judicial es avasalladora, haciéndose complicado localizar de forma eficiente y congruente la información jurídica útil en un momento determinado.

El desarrollo de la jurismática en Estados Unidos y Europa comienza en 1960, pero no es hasta 1980 cuando se le otorga relevancia en México; actuando como importante órgano iniciador, el Instituto de Investigaciones Jurídicas de la UNAM. Así, nuestro país ingreso a los países para los cuales el empleo de la informática jurídica se hace de forma cotidiana e incluso a llegado a considerarse como imprescindible.

2.1.1. Historia.

El uso de computadoras como herramienta del Derecho inició en Estados Unidos en 1949, cuando el juez Lee Loevinger -responsable de la División de Antitrust- escribió dos artículos: el primero denominado “The next step forward (El siguiente paso hacia el futuro)”, publicado en la Revista Minnesota Law Review, y el segundo titulado “Science and Prediction in the Field of Law (Ciencia y predicción en el ámbito de la ley)”. Artículos en los que estudió a una nueva disciplina, a la que llamó “jurimetría”. La jurimetría tendría por objeto la investigación científica de los problemas jurídicos, la racionalización del Derecho por medio de la aplicación de la metodología simbólica, y el empleo de los métodos cuantitativos de la automatización.

En 1959, en la Universidad de Pittsburgh, Pennsylvania el profesor John F. Harty convencido de la necesidad de encontrar una forma más efectiva para tener acceso a la información legal inició el uso de las computadoras con fines no únicamente matemáticos sino también lingüísticos, para lo cual implemento el sistema “batch”, caracterizado por la enorme cantidad de elementos que se pueden manejar en una sola operación. Este sistema se puede considerar como el primero de los grandes sistemas de información jurídica documental. Dicho sistema después de ser rediseñado se integró a la Corporación de Sistemas Aspen, la cual lo explotó comercialmente.

En los setenta se desarrollaron diversos sistemas aplicables a la informática jurídica, entre ellos destacaron la comercialización de sistemas de procesamiento de datos legislativos realizado por la Corporación Americana de Recuperación de Datos (1964); un sistema orientado hacia los abogados litigantes de la Corporación de Investigación Automatizada de la Barra de Ohio (OBAR en 1967); surgiendo en 1973 el sistema LEXIS como sucesor del OBAR; y el sistema IBM-TEXT-PAC y el STAIRS, de la IBM usados para el procesamiento de documentos.

En 1963, Hans Baade editó la obra “Jurimetrisc: the Methodology of Legal Inquiry (Jurismétrica: la metodología del cuestionamiento legal)”. Sin embargo, entre 1966 y 1969,

el término "jurismétrica" fue cambiado por "cibernética y Derecho" o "iuscibernética" como la denominó Mario Lozano, quien en 1968 consideró que la cibernética aplicada al Derecho contribuye tanto a la depuración cualitativa como cuantitativa de éste.

Para 1985 en todo el mundo se encontraban en funciones más de 100 bancos de datos en el campo del Derecho, entre ellos el sistema "batch", que permitía la búsqueda del texto y de las palabras ordenadas alfabéticamente en los archivos y que fue la base para el desarrollo de los sistemas on-line (1971-), caracterizados porque existe un "diálogo" entre el usuario y la computadora, y porque la información puede ser obtenida a distancia; los sistemas on-line evolucionados (1975-); y los sistemas expertos o inteligentes (1980-). En todos los sistemas se le dio relevancia a la resolución de problemas lingüísticos y sintácticos para hacer más eficaz la búsqueda. Asimismo, se han creado los llamados "bancos de segunda generación" que se encuentran limitados a un área jurídica, por lo que su utilidad se encuentra orientada a expertos en una materia determinada.

En América Latina, es Brasil el primero en realizar proyectos de informática jurídica, inaugurando en 1972 el Centro de Información y Procesamiento de Datos del Senado Federal (PRODASEN).

En 1980 comenzó a operar el Sistema Argentino de Informática Jurídica (SAIJ); y en 1981 nuestro país incursiona en la materia con el sistema UNAM-JURE, el cual no sólo es útil al investigador jurídico, sino que también aporta conocimientos e información a otros medios, entre ellos al gubernamental.

2.1.2. Contenido, concepto y clasificación.

La informática jurídica auxilia al jurista en la labor de investigación, otorgándole bancos de datos de los que gracias a la cantidad de información contenida se pueden obtener datos de alta precisión y calidad. Sin embargo, se debe reconocer que pueden existir fallas, pero éstas deben considerarse como "una molestia y no como un vicio redhibitorio".⁴ Dentro de esas fallas se encuentran algunas relativas a cualquier investigación, como el que en ocasiones la búsqueda puede conducirnos a documentos de poco interés y en otras dejar escapar información que se relacione directamente con el tema.

La informática jurídica es un instrumento de apoyo en el conocimiento y aplicación del Derecho, destacando su utilidad en la simplificación de información jurídica; el acceso generalizado de la población al conocimiento del Derecho; en la permanente actualización de los juristas; y en la superación de las limitaciones de la difusión de la información, otorgando acceso al Derecho internacional (incluso en el idioma nacional). "También existe una relación potencial entre la informática jurídica y la democracia, pues la información que es verdaderamente difundida redistribuye y equilibra el poder que corresponde a las personas y las instituciones en un sistema democrático".⁵

⁴ Fix Fierro, Héctor. Ob. cit., pág. 40.

⁵ Ibidem, pág. 110.

Existen numerosas definiciones de informática jurídica, la cual es difícil de definir dado su reciente surgimiento. Muchas de ellas se refieren a la ciencia o conjunto de técnicas del procesamiento automatizado de la información jurídica, y consideran a la informática jurídica como todo procesamiento electrónico de datos jurídicos, lo cual es erróneo. La informática jurídica implica el empleo de conocimientos informáticos y jurídicos, siendo algunas definiciones acertadas las siguientes:

La informática jurídica en un inicio pudiera decirse que se trata de la utilización de las computadoras en el ámbito jurídico, pero un estudio más detallado nos lleva a definirla en términos generales como “la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática en general, aplicables a la recuperación de la información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación”,⁶ o como “el conjunto de estudios e instrumentos derivados de la aplicación de la informática al Derecho, o más precisamente, a los procesos de creación, aplicación y conocimiento del Derecho”. Aunque se debe manifestar que una definición más estricta excluiría a aquellas aplicaciones que no exigen una labor de concepción y desarrollo desde el punto de vista jurídico, como en el caso del uso de procesadores de textos en oficinas de abogados.⁷

La informática jurídica se desarrolla a través de dos instrumentos lingüísticos: El léxico y el thesaurus. Para el autor Juan José Ríos Estavillo, el léxico es la agrupación de palabras contenidas en cada uno de los documentos de un banco de información, que organizados, constituye la base documental; su función es organizar y dar estructura a las ocurrencias de palabras en la totalidad de los documentos, para resolver algunos problemas lingüísticos, gramaticales y morfológicos. Por su parte el thesaurus es el conjunto de conceptos de un área del conocimiento determinada relacionados por su significado.⁸

Como antes se especificó la informática jurídica, inicialmente surgió como informática documentaria de carácter jurídico, pero continuó su evolución, por lo que actualmente es clasificada en función de sus distintas aplicaciones y de su momento de origen en: Informática jurídica documental, informática jurídica de control y de gestión, e informática jurídica metadocumental.

2.1.2.1. Informática jurídica documental.

La informática jurídica documental (almacenamiento y recuperación de textos jurídicos), es el área más antigua de la informática jurídica y consiste en encontrar lo más rápido y pertinentemente posible la información almacenada. Abarca la creación, almacenamiento y recuperación de textos jurídicos relevantes, para lo que se crean bancos de datos documentales relativos a cualquiera de las fuentes del Derecho (excepto de la

⁶ Téllez Valdés, Julio. Ob. cit., pág. 26.

⁷ Fix Fierro, Héctor. Ob. cit., pág. 56.

⁸ Ríos Estavillo, Juan José. Ob. cit., pág. 48.

costumbre) a efecto de interrogarlo con base en criterios propios basados en la información y en su relevancia jurídica.

Así, el proceso incluye entre otros, la recolección, organización, almacenamiento, recuperación, interpretación y uso de la información, por lo que se combinan la utilización de técnicas documentales y técnicas informáticas.

Dentro de los métodos de almacenamiento de datos jurídicos se encuentran:

- ◆ El full-text. En él se introducen los textos íntegros en la memoria de la computadora, y
- ◆ El key word o método de indización. En el cual de forma previa se analiza el documento para extraer y concretar sus características fundamentales, obteniéndose de cada documento un resumen o *abstract*. Hoy en día existen dos tipos de *abstracts* jurídicos fundamentales: el legislativo y el jurisprudencial.

En la actualidad los sistemas más importantes para la información jurídica documental son:

En Alemania:

JURIS, del Ministerio de Justicia de la República Federal Alemana.

DATEV, Sistema de acceso privado.

En Bélgica:

CREDOC, patrocinado por la Federación Real de Abogados y Notarios.

En Brasil:

PRODASEN, de la Cámara de Senadores de Brasil.

En Estados Unidos:

LEXIS, de la compañía Mead Data Central. Sistema comercial.

WESTLAW, de la West Publishing Company. Sistema comercial.

AUTO-CITE, de la Lawyer's Cooperative Publishing Company.

JURIS, del Departamento de Justicia. Sistema público.

FLITE (Federal Legal Information Through Electronics -Información legal federal a través de la electrónica-), de la Air Force Accounting and Finance Center. Sistema público.

En Francia:

IRETIJ, del Instituto de Investigación y Estudio para el Tratamiento de la Información Jurídica.

CEDIJ, del Consejo de Estado y el Tribunal Supremo.

CRIDON, del Centro de Investigación en Materia de Documentación Notarial.

En Inglaterra:

EUROLEX, servicio comercial.

En Italia:

ITALGIURE FIND, de la Suprema Corte de Casación.

IDG, del Instituto para la Documentación Jurídica de Florencia.

En México:

UNAM-JURE, del Instituto de Investigaciones Jurídicas de la UNAM.

CILSEN (Centro de Informática Legislativa del Senado de la República), de la H. Cámara de Senadores.

SCJ, de la Suprema Corte de Justicia.

SILE (Sistema de Información Legislativa), de la H. Cámara de Diputados.

En la Unión Económica Europea:

CELEX, de la Unión Económica Europea, con sede en Bruselas.

2.1.2.2. Informática jurídica de control y/o gestión.

La informática jurídica de control y/o de gestión y/o de administración (desarrollo de actividades jurídico-adjetivas) nace a fines de los sesenta y abarca principalmente los ámbitos jurídico-administrativo, judicial, registral y despachos de abogados. Implica el uso de computadoras para mejorar el proceso legislativo, así como los servicios de la administración pública, y de administración de justicia.

Trata de abarcar todo tipo de registros para brindar datos fehacientes, y facilitar la actuación en las oficinas relacionadas con el Derecho -públicas o privadas-, pudiendo realizar la computadora, a manera de ejemplo, toda actuación repetitiva. Su uso en la administración pública se da para recibir, tramitar, analizar y difundir información jurídica, entre otras; lo que conduce a su correcto funcionamiento al agilizar los trámites y disminuir la "inercia burocrática y corrupción".⁹ Así, puede utilizarse para la aceptación, registro e indicación de competencia y seguimiento de los expedientes judiciales de forma automática, donde la computadora incluso verifica si existe conexidad de causa.

En nuestro país el sistema que mejor representa esta actividad es el utilizado para la tramitación de las averiguaciones previas por la Procuraduría General de la República y la Procuraduría de Justicia del Distrito Federal, aunque también es de nombrarse la tramitación automatizada de los expedientes judiciales realizada por la Suprema Corte de Justicia de la Nación.

2.1.2.3. Informática jurídica metadocumental.

La informática jurídica auxiliar o metadocumental es prometedora, aunque todavía criticada debido a que utiliza la inteligencia artificial con el propósito de que la computadora auxilie para resolver o incluso resuelva por sí misma problemas jurídicos.

En tiempo reciente se pusieron en funcionamiento diversos proyectos prácticos, siendo de los más conocidos los sistemas de enseñanza del Derecho asistidos por computadora, y los sistemas expertos; éstos últimos se caracterizan por poder aprender.

Los sistemas expertos pueden realizar operaciones lógicas sobre una base de datos estructurada, por lo que es de suma importancia que dicha base contenga información confiable. Un sistema experto se encuentra conformado por los hechos o base de

⁹ Téllez Valdés, Julio. Ob. cit., pág. 42.

conocimientos en forma de base de datos, la interfase para lograr la comunicación entre el usuario y la computadora, y la heurística que es el método de inferencias lógicas que se aplica a la inteligencia artificial¹⁰ para obtener una decisión razonada.

Por ello, la doctrina considera que estos sistemas consisten en la estructuración de conocimientos especializados, que acoplados a un "mecanismo de inferencia", obtienen "conclusiones" a partir de la información que se les suministra en forma de preguntas y respuestas. Antonio Anselmo Martino define a un sistema experto como "aquél que, partiendo de ciertas informaciones proporcionadas por un especialista en la materia considerada, pretende resolver problemas que se presentan al interior de un específico "dominio" mediante la simulación de razonamientos que expertos han obtenido por sus conocimientos y sus experiencia adquiridas".¹¹ Entre los sistemas expertos con función jurídica encontramos el Taxman II de McCarty y Sheridan, y el de la Rand Corporation de Waterman y Peterson.

La informática jurídica metadocumental tiene injerencia en diversos ámbitos los cuales se pueden agrupar en cinco rubros:

- ◆ De ayuda a la decisión o informática jurídica decisional. El sistema no tiene que tomar la decisión, por lo general sólo auxilia para que ésta se tome; más que tomar las decisiones otorga un punto de partida al pensamiento humano. Aquí entran en práctica los sistemas expertos.
- ◆ De ayuda en la investigación o informática jurídica analítica. Se utiliza para poner a prueba hipótesis y teorías jurídicas susceptibles de ser enunciadas de modo riguroso y paso a paso para hallar la solución más razonable; se usa para "repensar" el Derecho. Es una de las áreas de la informática jurídica metadocumentaria que aún se encuentra en proceso de aplicación efectiva.
- ◆ De ayuda en la educación. Abarca la enseñanza asistida por computadora, donde se recalca que la enseñanza del Derecho puede ser mejor efectuada usando el apoyo en soportes informáticos. En este caso el sistema es usado con el fin de transmitir conocimiento jurídico, surgiendo este sistema como una importante herramienta para una mayor difusión y efectivización de la actividad docente.
- ◆ De ayuda en la previsión. A través del análisis factorial, la computadora ayuda en el análisis de bancos de datos multidimensionales que corresponden a una serie de caracteres, permitiendo que de forma apriorística se forme una conclusión basada en el análisis explicativo de los datos que se le dieron al ordenador. Se puede prevenir una consecuencia o predecir otras.
- ◆ De ayuda en la redacción. Se basa en programas que no sólo abarcan la forma del texto, sino que también, realizan correcciones de fondo, brindando un apoyo informático permanente al momento de la creación del texto (texto de Ley esencialmente). Las correcciones de fondo se llevan a cabo en base a la estructura lógica del texto, siendo

¹⁰ Charniak y McDermott definen a la inteligencia artificial como "el estudio de facultades mentales a través del uso de modelos computacionales". Citados por Ríos Estavillo, Juan José. Ob. cit., pág. 63.

¹¹ *Ibidem*, pág. 62.

principalmente utilizado para que el ordenador capte redundancias, lagunas y contradicciones, entre otras, obteniendo un texto ajustado a las intenciones legislativas.

2.1.3. Informática legislativa y judicial.

Fue en la Biblioteca del Congreso de Estados Unidos, en 1969 cuando se dio la primera aplicación experimental del uso de un ordenador electrónico para auxiliar en las funciones bibliotecarias. A partir de ese momento este uso se extendió en el mundo.

Sin embargo, en 1978 fue cuando en el servicio público del Senado francés, por medio de bases de datos, se difundió el uso de computadoras para labores específicas relativas a la actividad jurídica y legislativa. Desde entonces el avance tecnológico en hardware y software aplicable a éstas actividades no se ha detenido; se han generado centros de documentación jurídica, legislativa, parlamentaria y de ordenamiento de la jurisprudencia.

En los ochenta, numeroso países se integraron activamente a la informática parlamentaria; entre ellos: Australia, Bélgica, Dinamarca, Finlandia, Israel, Italia, y los Países Bajos.

En México fue en 1985 cuando nuestro Poder Legislativo inició el empleo de la informática legislativa.

La informática jurídica como instrumento al servicio de la función legislativa se ha amoldado a las necesidades específicas de los legisladores y de las propias asambleas legislativas. Ha brindado bancos de datos jurídicos actualizados (recuperación de información), así como de otras disciplinas para obtener un tratamiento interdisciplinario; sistemas expertos; y el empleo de la computadora en diversas funciones legislativas (por ejemplo, procesadores de palabras); entre otras.

En cuanto a la aplicación del Derecho por los tribunales, la informática jurídica le brinda al juez acceso a doctrina y al Derecho legislado en su contexto sistemático, además de que en cuanto a jurisprudencia se refiere, agiliza su localización y otorga una actualización constante. Asimismo, otorga a las partes que intervienen en un proceso, acceso a lo antes mencionado permitiéndole al abogado utilizar menos tiempo en la investigación y más tiempo en el razonamiento.

Declaraciones y documentos hispanos de carácter internacional han surgido de las reuniones entre legisladores y expertos en política científica para sentar las bases para la aplicación, el desarrollo y el uso de la informática en el Poder Legislativo y Judicial. Entre ellos destacan la Declaración de Salamanca, que surgió como consecuencia de los trabajos realizados durante la primera reunión de Parlamentarios Iberoamericanos sobre Ciencia y Tecnología (Madrid-Salamanca, 16 de noviembre de 1985); los trabajos realizados en la Reunión Latinoamericana de Legisladores pertenecientes a las comisiones de ciencia y tecnología de todos los países del área (Buenos Aires, 1987); y el Documento denominado "Investigación, Desarrollo e Industria" emanado de la Reunión Latinoamericana de Buenos

Aires, sobre Desarrollo Apoyado en la Ciencia y en la Tecnología. En todos se trató la transferencia de tecnología¹² y se llegó a conclusiones similares.

En la Declaración de Salamanca con la participación de países de América Latina, España y Portugal, se establecieron numerosas consideraciones, entre las que destaca que los parlamentos de los respectivos países deben desempeñar un papel decisivo en la definición de una política científica y tecnológica acorde con las necesidades sociales, y con las posibilidades y exigencias de nuestro tiempo. Por ello, se hicieron, entre otras, las siguientes recomendaciones:

- ♦ Que en todos los países iberoamericanos se adopten medidas explícitamente orientadas a la organización y adecuada operación de los respectivos sistemas de ciencia y tecnología, garantizando la máxima coordinación de esfuerzos y optimización de recursos de cada país.
- ♦ Que los parlamentarios promuevan la promulgación, reformas o adecuación del marco normativo que se relaciona con la ciencia y la tecnología en sus respectivos países, para favorecer su fomento, desarrollo y continuidad y que, de conformidad con sus atribuciones, estimulen la cooperación internacional y la vigencia de los convenios en la materia.
- ♦ Que los parlamentos presten especial atención a las repercusiones sobre el desarrollo científico y tecnológico implícitas en cualesquiera decisiones y normas legales de carácter económico, financiero, industrial, educativo, comercial y laboral.
- ♦ Que se constituyan en todos los parlamentos comisiones de ciencia y tecnología.
- ♦ Que con objeto de superar los desequilibrios intraregionales en esta materia, los diferentes organismos e instituciones nacionales e internacionales, incrementen los esfuerzos y acciones tendientes a promover un desarrollo equilibrado, homogéneo y complementario entre los diferentes países de la región.

De los trabajos realizados en la Reunión Latinoamericana de Legisladores pertenecientes a las comisiones de ciencia y tecnología de todos los países del área surgió un documento en el que se plasmaron, por ejemplo, las siguientes consideraciones:

- ♦ Los países desarrollados al ser los poseedores de nuevas tecnologías tratan de monopolizarlas y de usarlas con el propósito de conservar privilegios; crear dependencia y dominar política, económica y culturalmente a otras naciones. Por lo que es fundamental que los países latinoamericanos posean capacidad de dominio sobre tecnologías que puedan ser empleadas para dar solución a los problemas prioritarios nacionales. Sin embargo, siendo casi imposible sustentar el desarrollo tecnológico de un país en tecnología autónoma surge la necesidad de la transferencia de tecnología, y con ella la de lograr una integración latinoamericana para alcanzar objetivos de autonomía; y

¹² En opinión del Ingeniero Padilla Segura la transferencia de tecnología no se efectúa en el momento en que se ha instalado una línea de producción que da como resultado bienes que sustituyen a los que con anterioridad se importaban, sino cuando una persona física o moral está dispuesta a enseñar cómo hacer los bienes en calidad, cantidad, permanencia en la producción y con todas las características que los hagan competitivos en cualquier mercado, tanto por su precio como por su calidad y por la infraestructura de servicios que pueden ofrecer. Padilla Segura, José Antonio. Ob. cit., pág. 136.

♦ En cuanto a los servicios informáticos deben establecerse reglas comunes y claras para el flujo de datos transfronteriza, permitiéndose el transferir información y el procesamiento a distancia con base en normas convenidas de mutuo acuerdo.

Por su parte, en el Documento "Investigación, Desarrollo e Industria" emanado de la Reunión Latinoamericana de Buenos Aires, sobre Desarrollo Apoyado en la Ciencia y en la Tecnología, se trataron numerosos temas, siendo uno de ellos el de la informática.

Con respecto a la informática se indicó que ésta se apoya básicamente en la electrónica, las telecomunicaciones y los sistemas, por lo que estas áreas deben desarrollarse armónicamente y de manera integrada; además, de que considerando que el desarrollo de la informática es un objetivo estratégico, el Estado deberá jugar un papel destacado en la orientación, promoción, y ejecución directa de su desarrollo.

En el mismo documento se estableció que una política nacional en el área de la informática, debería asentarse, principalmente, sobre las siguientes consideraciones:

♦ La tecnología informática puede contribuir decisivamente al mejoramiento económico y social del país a través de su aplicación en la producción y los servicios; de su empleo en la gestión administrativa; y de sus efectos sobre el desarrollo de la ciencia, la integración del país, y el acceso a la educación y la cultura.

♦ Los Estados de la región, deberían considerar la posibilidad de hacerse cargo de la investigación y el desarrollo en las áreas de interés nacional con alto riesgo tecnológico, asimismo, deberían considerar programas de cooperación entre dichos países para la investigación, y el desarrollo tecnológico y de recursos humanos.

♦ La informática debe servir para satisfacer necesidades y no para crearlas; y

♦ Los Estados, como lo han hecho en los países que han avanzado en este sector, deberían crear el marco de políticas económicas, científicas y tecnológicas aptas para favorecer un desarrollo productivo nacional que tienda a la autonomía tecnológica en el campo de la informática, sin que ello implique buscar como objetivo la autarquía a la autosuficiencia en esa área.

2.2. El Derecho de la informática.

Numerosas nomenclaturas se han utilizado para denominar a la convergencia de dos ciencias; Derecho e informática, por ejemplo, en el Consejo de Europa (30 de abril de 1980) se recomendó que se le reconociera como "Derecho e informática"; sin embargo, hasta el momento, el término que ha gozado de mayor reconocimiento es "Derecho de la informática".

Hace varios años la influencia de la informática en el campo jurídico era todavía algo ilusorio y no se podía concebir mucho menos que el Derecho regularía a la informática.

Pero, en nuestros días la utilización de la informática como herramienta del jurista ha dado origen a la informática jurídica; y la aplicación de la informática en la actividad humana también ha originado una serie de situaciones que deben ser reguladas por la Ley.

El Derecho es producto de la organización social y es esencial para hacer posible la convivencia humana, por lo que como el maestro Legaz Lacambra manifestó: el Derecho "es una forma necesaria del vivir social, lo mismo que el vivir social es una forma inherente a la existencia humana: donde hay hombre hay sociedad y donde existe ésta, debe haber un Derecho",¹³ y en el mismo sentido el maestro Villoro Toranzo define al Derecho como el "sistema racional de normas sociales de conducta, declaradas obligatorias por la autoridad, por considerarlas soluciones justas a los problemas surgidos de la realidad histórica".¹⁴

La informática se ha convertido en parte de nuestra realidad social al permitir el tratamiento automatizado de enormes cúmulos de información; surgiendo el Derecho de la informática como respuesta social a la "Revolución Digital".

El Derecho de la informática ha sido definido por diversos autores. Para Carrascosa López, es el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones.¹⁵ Para Emilio Suñe, es el conjunto de normas reguladoras del objeto informática o de problemas directamente relacionados con la misma.¹⁶ Para Juan José Ríos Estavillo, es el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas.¹⁷ Y Para Julio Téllez, es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática. Es un conjunto de leyes en cuanto que, si bien escasos, existen varios ordenamientos jurídicos nacionales e internacionales con alusión específica al fenómeno informático. Normas en virtud de aquellas que integran la llamada política informática.¹⁸ Principios en función de aquellos postulados emitidos por jueces, magistrados, tratadistas y estudiosos respecto al tema. Hechos, como resultado de un fenómeno aparejado a la informática, es decir, no imputables al hombre. Y por último, actos, como resultado de un fenómeno directamente vinculado a la informática y provocado por el hombre.¹⁹

¹³ Citado por Téllez Valdés, Julio Ob. cit., pág. 19.

¹⁴ Ibidem, pág. 20.

¹⁵ Citado por Ríos Estavillo, Juan José. Ob. cit., pág. 73.

¹⁶ Idem.

¹⁷ Idem.

¹⁸ Para este autor la política informática consiste en las normas necesarias para llevar a cabo una planificación tendiente al desarrollo informático adecuado, siendo la política diferente a la legislación informática, en cuanto, a que esta última se refiere a aspectos más específicos al ser un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso (fundamentalmente inadecuado) de la informática. Téllez Valdés, Julio. Ob. cit., pág. 59.

¹⁹ Ibidem, pág. 58.

Sin embargo, la doctrina aún no ha logrado llegar a un acuerdo en cuanto si al Derecho de la informática se le debe reconocer o no como una rama autónoma en el campo del Derecho, por lo que se ha preferido determinar ciertos campos de estudio como aquéllos en los que resulta de mayor relevancia determinar la regulación aplicable cuando la utilización de la informática acarree consecuencias jurídicas. Estos campos son:

- ◆ Los delitos informáticos;
- ◆ El flujo de datos transfrontera;
- ◆ La protección jurídica del software;
- ◆ Los convenios o contratos informáticos;
- ◆ La protección jurídica de los datos personales y, en general, el derecho de acceso a la información;
- ◆ Las condiciones de trabajo relacionadas con el uso de computadoras o ergonomía informática; y
- ◆ Los problemas jurídicos derivados de la naturaleza de los nuevos soportes de información, incluyendo el estudio del valor probatorio de los documentos electromagnéticos.

2.3. Normatividad de la informática en México.

Por desgracia no fue sino hasta finales de los sesenta que empezaron a surgir inquietudes sobre las repercusiones de la "Revolución Informática" en el Derecho, surgiendo en Francia la Comisión Nacional de Informática y Libertades para proteger las libertades individuales y sociales que pudieran verse amenazadas a causa del creciente avance tecnológico; a partir de ese momento se hizo cada vez más evidente la necesidad de que el estudio de los juristas abarcará tanto a las situaciones ya existentes relativas al desarrollo de la informática, como a las que puedan surgir, a fin de establecer un marco normativo para esta ciencia.

Sin embargo, en nuestro país aún hoy existe muy poca legislación relativa a esta materia, surgiendo la urgencia de legislar al respecto.

2.3.1. Marco normativo de la informática en nuestro país.

En 1984 la Gran Comisión del Senado de la República encomendó a su Comisión Especial de Informática, entre otras cuestiones, identificar las necesidades de legislación en esta materia y, en su caso; proponer criterios y bases generales para establecer un marco normativo, formular los proyectos de iniciativa correspondientes, y estudiar la conveniencia de establecer un Centro de Informática Legislativa como órgano del Senado.

Derivado de lo anterior el Centro de Informática Legislativa del Senado (CILSEN) inició sus operaciones a partir del 7 de octubre de 1986; y como resultado del trabajo encomendado a la Comisión Especial de Informática, ésta definió los criterios fundamentales para establecer un marco normativo aplicable a la informática. La Comisión concluyó, que con base en el régimen de competencias establecido en el artículo

124 de nuestra Carta Magna, ya que la facultad para legislar en materia de informática no se encuentra expresamente concedida a la Federación, debe entenderse reservada a los Estados.

Tomando en cuenta tan importante conclusión de la Comisión, el CILSEN profundizó en los estudios con el propósito de proponer la forma de legislar a nivel constitucional sobre informática; de tal esfuerzo se obtuvo el documento titulado "Marco normativo de la Informática en México". En este documento se plasman estudios normativos sobre el artículo 73 constitucional, y los artículos 6, 26, 28, y 134 de nuestra Carta Magna; éstos últimos se incluyeron debido a que de ellos se desprenden implicaciones de índole informática en cuanto a la información, planeación, actividades estratégicas y adquisiciones de equipo, entre otros.

En cuanto a la legislación ordinaria, la investigación abarcó aquellas leyes que influyen en áreas que regulan aspectos de la informática relacionados con telecomunicaciones o respecto de su propio desarrollo como tecnología; o que tratan de la informática como instrumento y función de la información; o que se refieran a la informática y a la electrónica como medios de producción de bienes y servicios o bien como productos tecnológicos en sí mismos; o finalmente, que regulen la propiedad industrial del soporte lógico. Por último, en cuanto a los convenios internacionales se incluyeron sólo aquéllos que vinculan la informática con las telecomunicaciones.

Asimismo, el estudio realizado nuevamente hizo evidente la existencia de un vacío legislativo en el orden federal mexicano respecto de la informática, proponiéndose, en un principio, como solución, adicionar la fracción X del artículo 73 constitucional con la palabra "informática", y señalar las áreas específicas sobre las que el Congreso de la Unión debería legislar, a saber: Garantías individuales, sociales y políticas; seguridad nacional; soberanía nacional; flujo de datos transfrontera; delitos informáticos; protección a la propiedad intelectual sobre programas de computadoras; promoción del desarrollo científico; promoción de la enseñanza de la informática en los niveles de educación básica y formación de profesionistas e investigadores; y defensa de nuestros valores culturales.

El documento "Marco normativo de la Informática en México"²⁰ se dividió en tres títulos denominados:

A) Estado actual de la normatividad sobre informática en México Este título se subdivide en:

1.- Legislación relacionada con la informática. Comprende aquellas normas que a pesar de no mencionar expresamente la palabra "informática", son aplicables en las circunstancias en que esta tecnología está presente.

2.- Legislación específica sobre informática. Se integra con las normas que de manera expresa mencionan el término "informática";

²⁰ Padilla Segura, José Antonio. Ob. cit., p.p. 9 a 42.

B) Proyecto de exposición de motivos sobre la necesidad de establecer un marco normativo en materia de informática; y

C) Proyecto por el que se adiciona la palabra "informática" a la fracción X del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos.

Siendo el contenido de cada uno de ellos el siguiente:

A) Estado actual de la normatividad sobre informática en México.

En este título se realizó el estudio de los siguientes artículos y legislación:

* Artículo 6 constitucional. En él se establece como garantía constitucional, el derecho a la información²¹, al indicar que "el derecho a la información será garantizado por el Estado".

El concepto de derecho a la información apareció formalmente en la Declaración Universal de los Derechos del Hombre de 1948, y es considerado por la doctrina como el derecho a ser informado a través de los medios de comunicación con veracidad, objetividad y oportunidad, así como el derecho de obtener el acceso a dichos medios.²² Comprende el difundir, investigar y recibir información, es decir, abarca el deber de informar y el derecho a ser informado.²³

* Artículo 26 constitucional. Este artículo establece el sistema de planeación nacional, el cual está a cargo del Estado, incluyéndose dentro de este sistema a la tecnología informática como uno de los temas prioritarios de investigación, de conformidad con lo establecido en el Plan Nacional de Desarrollo. El Estado considera a la informática como el medio promotor de tecnologías que coadyuvarán al crecimiento de la economía nacional para la independencia y la democratización política, social y cultural de la nación.

* Artículo 28 constitucional. El Estado se reserva el ejercicio exclusivo de ciertas áreas estratégicas de actividades, por su importancia y trascendencia para la vida nacional. El Estado es el facultado para crear los organismos y empresas que se requieran para el eficaz manejo de las mismas; encontrándose expresamente dentro de esas áreas la comunicación vía satélite.²⁴

²¹ El autor Juan José Ríos Estavillo indica que es necesario distinguir entre el derecho a la información y el derecho de la información o sobre la información, ya que el primero es un derecho constitucional por medio del cual se garantiza que el gobernado esté debidamente enterado de los diversos factores de índole social, político y económico que se realicen en la sociedad y que afecten o no la misma; mientras que el segundo es el conjunto de normas jurídicas que tienen como fin fundamental llevar el control del uso, goce y disfrute de un bien inmaterial resultado del proceso social que es la información. Ríos Estavillo, Juan José. Ob. cit., pág. 25.

²² Padilla Segura, José Antonio. Ob. cit., pág. 12.

²³ El deber de informar implica al derecho de expresión y al acceso a fuentes de información pública así como a los medios de comunicación. Mientras que el derecho a ser informado se refiere al derecho de ser informado de todo lo que afecte la existencia de una persona en particular. Téllez Valdés, Julio. Ob. cit., pág. 66.

²⁴ Al respecto, es importante tener en consideración a los artículos 11, 326, 377, 380, 386, 533, y 571 de la Ley de Vías Generales de Comunicación; así como al Reglamento de este ordenamiento legal.

Este tipo de comunicación es utilizada para transmitir cualquier clase información, siendo un medio propicio para la comisión de delitos como el robo de programas de cómputo, o la violación a la confidencialidad de la información. La comunicación vía satélite también aparece importantes consideraciones con respecto a la teleinformática.

* Artículo 134 constitucional. En este artículo se establecen los principios del sistema legal de administración de los recursos económicos del Gobierno Federal, del Distrito Federal y las entidades paraestatales, a saber, eficiencia, honradez e idoneidad en el gasto. Para lograr la efectividad de dichos principios se sujeta a las adquisiciones, arrendamientos, prestación de servicios, obras, y enajenaciones de todo tipo realizadas por dichas dependencias a la licitación pública; aunque se admiten excepciones en el caso de que dicho procedimiento no sea el más idóneo según el caso. De lo anterior el autor Padilla Segura infiere que bajo tales principios habrán de concertarse las adquisiciones de equipo y la administración de los bienes informáticos.²⁵

* Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles (D.O.F. 8 de febrero de 1985).

* Ley sobre el Control y Registro de la Transferencia de Tecnología y el Uso y Explotación de Patentes y Marcas (D.O.F. 11 de enero de 1982). Arts. 2, y 5.

* Ley para Coordinar y Promover el Desarrollo Científico y Tecnológico (D.O.F. 21 de enero de 1985).

* Ley de Información Estadística y Geográfica (D.O.F. 30 de diciembre de 1980; y adiciones D.O.F. 12 de diciembre de 1983). Arts. 2-V; 3-VII; 30-VI, VII, VIII; 33; y 34.

* Ley de Invenciones y Marcas (D.O.F. 10 de febrero de 1976). Art. 9-III.

* Ley Orgánica de la Administración Pública (D.O.F. 29 de diciembre de 1976). Arts. 20; 32-XVII; 34-XII; 36-I a III, XII, XIII, XV, XVII; y 38-VIII.

* Ley de Presupuesto, Contabilidad y Gasto Público Federal (D.O.F. 31 de diciembre de 1976). Art. 7.

* Ley para Promover la Inversión Mexicana y Regular la Inversión Extranjera (D.O.F. 9 de marzo de 1973). Art. 13.

* Reglamento Interior de la Secretaría de Programación y Presupuesto (D.O.F. 29 de julio de 1985). Arts. 25, 26-III, y 28.

* Reglamento de la Ley de Información Estadística y Geográfica (D.O.F. 3 de noviembre de 1982). Art. 59.

* Reglamento de la Ley de Presupuesto, Contabilidad y Gasto Público Federal (D.O.F. 18 de noviembre de 1981). Art. 72-III.

* Reglamento del Registro Público de la Propiedad y del Comercio del Departamento del Distrito Federal (D.O.F. 6 de mayo de 1980). Art. 126.

* Reglamento de la Ley sobre el Control y Registro de la Transferencia de Tecnología y el Uso y Explotación de Patentes y Marcas (D.O.F. 25 de noviembre de 1982). Arts. 20 al 29.

* Acuerdo por el que se Crea la Comisión de Informática del Departamento del Distrito Federal (D.O.F. 24 de diciembre de 1984).

²⁵ Padilla Segura, José Antonio. Ob. cit., pág. 17.

- * Acuerdo por el que se Determina que la Comisión de Informática del Departamento del Distrito Federal seguirá Funcionando (D.O.F. 5 de junio de 1986).
- * Acuerdo 114 por el que se Dispone que los Programas de Computación podrán Inscribirse en el Registro Público del Derecho de Autor (D.O.F. 8 de octubre de 1984).
- * Acuerdo por el que la Secretaría de Programación y Presupuesto dictará las Medidas Necesarias para Coordinar las Tareas de Informática que Desarrollen las Dependencias y Entidades de la Administración Pública Federal (D.O.F. 16 de enero de 1978).
- * Convenio sobre la Distribución de Señales Portadoras de Programas Transmitidos por Satélite (D.O.F. 6 de febrero de 1976).
- * Convenio de la Red de Información Tecnológica Latinoamericana (D.O.F. 20 de diciembre de 1984 y 6 de mayo de 1985).
- * Reglamento de Radiocomunicaciones derivado de la Unión Internacional de Telecomunicaciones.

B) Proyecto de exposición de motivos sobre la necesidad de establecer un marco normativo en materia de informática.

Hoy la sociedad atesora información útil y la considera un insumo básico intangible, cuyo tráfico en cantidad ha igualado a la del transporte. La informática ya se emplea en el quehacer público; y para el legislador constituye una herramienta indispensable para el almacenamiento, procesamiento y recuperación de la información necesaria para realizar su labor.

Los actuales poseedores de información, y comunes instrumentadores de la informática han alcanzado poder económico y político de gran magnitud, siendo imprescindible para los Estados y sus gobiernos, asumir posiciones y definir criterios sobre ciencia, tecnología e informática, siempre teniendo en cuenta los objetivos nacionales.

En los países desarrollados, a las materias antes mencionadas se les ha considerado como materias de interés nacional, debido a que no han sido analizadas sólo en su aspecto técnico, sino que han considerado también la influencia que ejercen en la vida nacional, su capacidad para promover transformaciones sociales, y la necesidad de que la información sea un recurso que esté al alcance y servicio de la sociedad; en vez de que se convierta en instrumento para su sometimiento. Así, y de conformidad con el autor Padilla Segura²⁶ la informática debe ser considerada como actividad prioritaria del Estado, para lograr su efectiva promoción y desarrollo.

La existencia de un aparato científico y tecnológico nacional que sea compatible con las necesidades y el desarrollo del país, se traduce en la obtención de independencia política, la reducción de la dependencia económica y tecnológica, y la posibilidad del ejercicio cabal de la soberanía.

Por todo ello, el Senado Mexicano debe contar con las facultades para legislar en materia de informática; porque ya no se discute si la materia informática debe ser regulada, sino como normarla. El marco normativo de la informática debe ser muy prudente; no debe

²⁶ Idem.

implicar limitaciones o restricciones a su desarrollo, a la investigación, a la creatividad o a las actividades productivas de bienes o servicios informáticos, pero no se puede desvincular del marco constitucional, ni de las directrices que norman las relaciones internacionales; debe garantizar y proteger cabalmente los derechos y los valores fundamentales del hombre, de la familia, de la sociedad y de los países; y a toda costa debe evitarse su empleo indebido.

C) Proyecto por el que se adiciona la palabra “informática” a la fracción X del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos .

Anteproyecto de decreto por el que se adiciona la palabra “informática” a la fracción X del ARTÍCULO 73 de la Constitución Política de los Estados Unidos Mexicanos.²⁷

Primero. Que el Senado de la República está plenamente consciente de la necesidad de actualizar, enriquecer y consolidar la infraestructura jurídica que permita diseñar nuevas estrategias que conduzcan a nuestro país a su desarrollo integral, el cual está estrechamente ligado al progreso que se logre en el campo de la informática.

Segundo. Que la informática se ha convertido en factor primordial de la moderna organización social -cuyas modalidades debe adoptar oportunamente- a la cual nuestro país debe integrarse cada vez más estrechamente y que tal organización requiere del apoyo, del estímulo y de la orientación de todos sus miembros y, especialmente, del Estado.

Tercero. Que cada día resultan más evidentes, importantes y trascendentes las repercusiones de la informática en la configuración cultural de nuestro pueblo, por lo que es necesario adoptar las medidas pertinentes, entre ellas, las de orden jurídico, para defender y preservar ese patrimonio nacional que es base y componente indispensable para perdurar como nación independiente, cuyos valores y manifestaciones puedan trascender históricamente.

Cuarto. Que la complejidad de la informática y el hecho de que constituye un fenómeno de convergencia tecnológica hacen que influya en gran número de procesos técnicos, lo cual conduce a considerarla como una actividad de importancia nacional y prioritaria, ya que de lo contrario otras importantes áreas de actividad se verían seriamente afectadas.

Quinto. Que hasta hoy, el marco jurídico de la informática en nuestro país no ha logrado alcanzar una cabal unidad y coherencia, ya que está formada por disposiciones que se encuentran dispersas en distintos ordenamientos jurídicos y administrativos de donde se desprende la necesidad de expedir una legislación federal unificadora de las políticas y de los criterios relativos.

Sexto. Que el fenómeno informático está presente no sólo en la gestión operativa de la empresa privada de nuestro país, sino también en los mecanismos de decisión política por lo cual resulta imprescindible normarla jurídicamente a fin de obtener las máximas ventajas de su uso intensivo.

²⁷ Ibidem, p.p. 37 y 38.

Séptimo. Que de acuerdo con nuestro régimen de competencias, consignado en el Artículo 124 constitucional, la facultad para legislar en materia de informática quedaría reservada a las entidades federativas, las cuales, hasta hoy, no han ejercido tal atribución.

Octavo. Que la facultad del Congreso de la Unión para legislar en materia informática no puede considerarse como implícita, ya que su objeto no se reduciría a hacer efectiva alguna otra otorgada por la Constitución, ni tampoco puede desprenderse de la fracción XXIX inciso "F", de la propia ley fundamental, puesto que el fenómeno informático asume características propias que lo hacen trascender, por sí mismo, en todos los ordenes del acontecer social.

Noveno. Que a fin de fortalecer el estado de derecho que prevalece en nuestro país es conveniente que se expida una legislación federal en materia informática a cuyo efecto resulta imprescindible facultar expresamente al Congreso de la Unión para legislar en dicha materia.

Décimo. Que la carencia de un marco jurídico integral sobre la informática ha dado lugar a que algunas dependencias de la administración pública federal hayan tenido que realizar acciones y tomar decisiones en esta materia.

Undécimo. Que de acuerdo con el artículo 73 constitucional, el Senado de la República es competente para presentar iniciativas de ley.

Se propone:

Establecer un régimen explícito de competencia en materia informática a nivel federal, mediante la adición de la palabra "informática" en el texto de la fracción X del Artículo 73 constitucional en los siguientes términos:

Decreto por el que se adiciona una palabra a la fracción X del Artículo 73 de la Constitución Política de los Estados Unidos Mexicanos:

DECRETO

El Congreso de los Estados Unidos Mexicanos en uso de la facultad que le confiere el artículo 135 de la Constitución General de la República y previa aprobación de la mayoría de las honorables legislaturas de los Estados, declara adicionado el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos.

Artículo único. Se adiciona la fracción X del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos para que dicha fracción quede en los siguientes términos:

X. "Para legislar en toda la República sobre hidrocarburos, minería, industria cinematográfica, comercio, juegos con apuestas y sorteos, servicios de banca y crédito, energía eléctrica y nuclear, informática, y para establecer el Banco de Emisión Único en los términos del artículo 28 y para expedir las leyes del trabajo reglamentarias del artículo 123."

2.4. Flujo de Datos Transfronterizos (FDT).

El problema del flujo de datos transfrontera, como consecuencia de la teleinformática, es uno de los que más preocupan a la comunidad internacional, al haberse dificultado el

control de los datos debido al incremento de la facilidad con que pueden entrar y salir de un país; facilidad proporcionada principalmente por el uso de redes.

Dentro de las redes más importantes se pueden mencionar a la Red Europea de Transmisiones (EURONET), que conecta bancos de información en Europa Occidental; la Red Bancaria de Intercambio de Mensajes Financieros (SWIFT); y en especial Internet, la cual no es propiedad exclusiva de nadie al funcionar por la colaboración técnica y administrativa entre diversas redes.

El Consejo Económico de la Organización de las Naciones Unidas define al Flujo de Datos Transfronterizos como "la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y recuperación".²⁸ Dicho flujo acarrea numerosas ventajas y por ello se ha incrementado su uso, pero también tiene aparejadas problemáticas jurídicas particulares, a saber: la utilización ilícita de datos transmitidos al extranjero, tarifas y régimen fiscal aplicables, atentado a la soberanía de los Estados, contratos informáticos, propiedad intelectual de la información, y delitos informáticos.

Cada problemática amerita un control jurídico, por lo que los sistemas jurídicos nacionales e internacionales deben ocuparse de su regulación, tomando en consideración que la "norma jurídica nacional velará por el cumplimiento de los esquemas de protección jurídica de la información nacional en correlación con la comunidad internacional y viceversa".²⁹

Por lo antes mencionado, diversos organismos se han dado a la tarea de regular jurídicamente el fenómeno provocado por el Flujo de Datos Transfronterizos, entre ellos podemos mencionar:

- ◆ A la Organización para la Cooperación del Desarrollo Económico (OCDE), la que con su Recomendación del 23 de septiembre de 1980 incursionó en el estudio de la problemática que se deriva de la protección y seguridad de datos;
- ◆ A la Comisión de Comercio y Desarrollo de las Naciones Unidas (UNCTAD), interesada en la problemática contractual y propiedad de la información;
- ◆ A la Oficina Intergubernamental para la Informática (IBI), que investiga las repercusiones generales y particulares del fenómeno del Flujo de Datos Transfronterizos;
- ◆ Al Acuerdo General para Aranceles y Tarifas (GATT), en lo referente a las tarifas y régimen fiscal aplicables; y
- ◆ Al Banco Mundial, en cuanto al derecho de la privacidad y confidencialidad de datos.

En México, se aplican además de todas las disposiciones mencionadas en el Capítulo II de la presente investigación relativas a la informática y a la información, entre otras:

²⁸ Téllez Valdés, Julio. Ob. cit., pág. 77.

²⁹ Ríos Estavillo, Juan José. Ob. cit., pág. 106.

- ◆ La Ley Federal de Radio y Televisión, en lo relativo a las limitantes en materia de transmisión de información;
- ◆ El Código Penal para el Distrito Federal;
- ◆ El Acuerdo que regula el establecimiento y operación de los sistemas de transmisión de señales de datos y su procesamiento por parte de la Secretaría de Comunicaciones y Transportes, en cuanto a los lineamientos técnicos; y
- ◆ El Tratado Trilateral de Libre Comercio de América del Norte (TLCAN), el cual en el Capítulo XIII, contiene disposiciones alusivas al tema, al referirse a las medidas que adopte o mantenga una parte, relacionadas con: el acceso y el uso de redes o servicios públicos de telecomunicaciones por personas de otra parte; el acceso y uso que dichas personas harán cuando operen redes privadas; la prestación de servicios mejorados o de valor agregado por personas de otra parte, en territorio de la primera o a través de sus fronteras; y la normalización respecto de la conexión de equipo terminal u otro equipo a las redes públicas de telecomunicaciones.

El TLCAN, asimismo, estipula que cada una de las partes deberá garantizar que personas de otra parte tengan acceso y puedan hacer uso de cualquier red o servicio público de telecomunicaciones ofrecidos en su territorio o de manera transfronteriza, en términos razonables y no discriminatorios, para la conducción de sus negocios; pero ninguna disposición se interpretará en el sentido de impedir a ninguna parte adoptar o aplicar cualquier medida necesaria para: asegurar la confidencialidad y la seguridad de los mensajes, o proteger la intimidad de los suscriptores de redes o de servicios públicos de telecomunicaciones.

2.4.1. Marco jurídico de Internet en los Estados Unidos Mexicanos.

La teleinformática, especialmente representada por Internet, es considerada como la tecnología gracias a la cual se lograrán enormes desarrollos sociales, y económicos en el siglo XXI; dado que el uso de Internet trae consigo el surgimiento de nuevas formas de interrelación humana. La Red permite que los países se encuentren cada vez más interconectados; surgiendo un fenómeno globalizador irreversible a nivel mundial que implica la afectación de diversas ramas del Derecho.

En nuestro país no existe una regulación expresa de Internet, por lo que su uso se ha basado, al igual que en casi todo el mundo, en la autorregulación y en los buenos modales cibernéticos reconocidos internacionalmente.

La autorregulación, en este caso, consiste en la elaboración de reglas voluntarias tipo estándar no creadas por el sistema legal sino por aquéllas que forman parte en la actividad que se realiza y que se someten voluntariamente a ellas. Una vez aceptadas las reglas, su desobediencia acarrea una pena.

Por su parte, los buenos modales o *cibermodales* consisten en simples reglas de cortesía, aunque su desobediencia también puede ser penalizada.

Como anteriormente se ha manifestado, para el jurista el surgimiento de nuevas tecnologías, como la teleinformática e Internet apareja la aparición de importantes herramientas a su servicio; pero al mismo tiempo surge la imperiosa necesidad de desarrollar una nueva legislación de acuerdo a los cambios que sufre la sociedad.

Antes de proseguir es necesario establecer una distinción entre la regulación de Internet como medio de comunicación, y la regulación de las consecuencias que produce.

La regulación de Internet como medio de comunicación ha tenido cierto rechazo al encontrarse entre los académicos opiniones encontradas. Unos sostienen que debe regularse como cualquier otro medio de comunicación, aunque no sea exactamente igual a ellos, ya que el Internet no sólo implica la transmisión de información sino también la interacción; mientras que los otros expresan que no debe existir regulación en absoluto. Los miembros de la academia que se muestran reticentes a la regulación basan sus consideraciones, fundamentalmente, en que dicha regulación muy probablemente conduciría a la censura electrónica, violando a la libertad de expresión, al derecho a la información, y a la propia forma de ser de la Red; ya que el derecho a la información es un aspecto de preponderante importancia en Internet, y en cuyo favor se ha manifestado la Suprema Corte estadounidense.

En nuestro país, la política institucional se ha manifestado a favor de la autorregulación; pero la mayoría de la doctrina mexicana considera que debe regularse y afirma, que si bien la autorregulación es positiva para la libertad de expresión, crea incertidumbre en cuanto se trata de la aplicación del Derecho.

En legislaturas pasadas se creó una comisión especial en la Cámara de Diputados denominada "Comisión Social", la cual estuvo relacionada con el estudio y probable regulación de Internet como un medio más de comunicación social. Pero, por razones que se consideran como políticas, toda vez que implica la regulación de la libertad de expresión, no fue un proyecto legislativo que haya tenido frutos.

Por su parte, Internet se encuentra en constante uso, lo que implica que a cada momento se están dando múltiples relaciones jurídicas. Pero, las consecuencias aparejadas al uso de Internet no constituyen un vacío regulatorio, ya que casi todas se pueden encuadrar en nuestra legislación; sin embargo, pocas de nuestras leyes resuelven de forma satisfactoria el empleo de las nuevas tecnologías.

En el ámbito jurisprudencial sí existe un vacío, que pudiera atribuirse a la relativamente reciente aparición de esta tecnología y a su incremento desmesurado.

Además, en México, uno de los mayores problemas lo constituye la falta de preparación informática en el Poder Legislativo y en el Poder Judicial.

Mundialmente los sistemas legales han tratado de regular las consecuencias derivadas del uso de la Red, y diversos organismos internacionales, como la OMC, y la OCDE, han tratado de regular jurídicamente a las redes. Desgraciadamente, en la mayoría de los casos

la legislación lograda a resultado incompleta y/o confusa al no poder abarcar todas las actividades desarrolladas en la Red. De lo anterior se desprende que existe un marco regulatorio aunque con variaciones nacionales y algunas lagunas legales.

Dentro de las lagunas legales, existen algunas que han obstaculizado la resolución de importantes problemas como el régimen aplicable a: los servicios ofrecidos en la Red, a la compra-venta a distancia, a la publicidad, a la prestación de servicios, a los proveedores de acceso, a la propiedad intelectual, al comercio electrónico, al documento electrónico como prueba, a la formación de contratos, al trabajo a distancia, a las transacciones electrónicas, a los delitos informáticos, y a la seguridad y confidencialidad dentro de la Red. Siendo estas las áreas que por su importancia necesitan de la determinación de un marco jurídico de forma inmediata.

Para lograr una adecuada legislación de la Red, en general, la regulación debe ser tolerante para permitir su crecimiento, y futurista para prever nuevas aplicaciones y sus repercusiones jurídicas. La legislación deberá asegurar la confidencialidad de la información (protección de la privacidad) y la seguridad; tomar en consideración a la autorregulación, a los *cibermodales*, y a leyes de otros países; deberá promover el desarrollo y el acceso general a la Red; y en especial, deberá tener en cuenta al funcionamiento propio de Internet donde, se respeta el derecho a la información, la libertad de expresión, y la diversidad de contenidos.

Además, no debe olvidarse que el funcionamiento de Internet es de carácter mundial, por lo que una marcada diferencia entre las regulaciones de los países, si bien no representaría ningún problema en el caso de la aplicación nacional, si pudiera disminuir notablemente los principales beneficios del uso de Internet a nivel Internacional.

En nuestro país, el uso de Internet se ha tenido que basar, principalmente, en los *cibermodales* y la autorregulación al existir numerosas lagunas legislativas al respecto. Ello no ha impedido que la cantidad de usuarios de la Red se incrementa día a día, ni que se use cotidianamente en operaciones en las que subyace una relación jurídica, como es el caso de la compra-venta de boletos, y en varios servicios financieros; a pesar de que la contratación vía Internet aún trae aparejados los riesgos de inseguridad y falta de confidencialidad.

En México, nuestros legisladores apenas están comenzando a reconocer la importancia de Internet, aunque su uso en nuestro país inició en los ochenta. Por ello los esfuerzos por legislar en la materia son dispersos, y se dirigen principalmente a la difusión y mejor uso de la informática, como lo demuestra el Decreto por el que se aprueba el Programa de Desarrollo Informático,³⁰ donde la política en materia informática dictada desde el Poder Ejecutivo Federal, se dirige a la promoción y al fomento de una nueva cultura de la educación a través de los medios informáticos.

Por su parte, la Ley Federal de Telecomunicaciones del 7 de junio de 1995, omite el concepto de Internet, sin embargo, la provisión de acceso al mismo puede encuadrarse

³⁰ Publicado en el Diario Oficial el 6 de mayo de 1996.

dentro de los servicios de valor agregado, al ser éstos definidos como los servicios que “presta un usuario de la red concesionada o red pública de telecomunicaciones, cuya actividad tiene efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida”, y por lo tanto, todo prestador de este servicio debe registrarse ante la Secretaría de Comunicaciones y Transportes (SCT).

Igualmente, en el Capítulo XIII del TLCAN, se considera la provisión de acceso a Internet como un servicio mejorado o de valor agregado, al involucrar aquellos servicios de telecomunicaciones que utilizan aplicaciones de procesamiento por computadora que: a) actúan en el formato, contenido, código, protocolo o aspectos similares de la información transmitida al cliente; b) proporcionan al cliente información adicional, diferente o reestructurada; o c) involucran interacción del cliente con la información almacenada.

CAPÍTULO

III

EL DOCUMENTO ELECTRÓNICO.

En nuestro actuar cotidiano el fenómeno de la informatización puede considerarse novedoso y con carácter irreversible, las computadoras permiten que se brinden servicios que antes eran inexistentes y se presentan como el medio idóneo de satisfacer necesidades sociales, en especial en el comercio y en los servicios financieros. Por lo que, muchas personas y en especial empresas sienten la necesidad de internarse en estos nuevos métodos tecnológicos, primordialmente en el Internet, para que sus competidores no los dejen relegados, aunque carezcan del conocimiento y de la infraestructura necesaria para hacerlo.

En nuestra realidad tenemos contacto constante con documentos electrónicos como son los tickets de compra y cualquier otro documento emitido por sistemas registrales automatizados como el recibo del agua, del teléfono, etcétera, por lo que no resulta difícil vislumbrar que en un futuro (tal vez demasiado cercano) casi toda la actividad de documentación se desarrollará a través de documentos electrónicos. La Administración Pública sería una de las más beneficiadas con su implementación al poder sustituir enormes cúmulos de información en soporte papel con pocos soportes magnéticos que contendrían aún mayor cantidad de información, y con ventajas que no otorgan los documentos en papel como una recuperación efectiva y rápida, bajo costo, y gran fidelidad; garantizando al igual que los documentos con soporte en papel su durabilidad.

A pesar de que el fenómeno informático avanza constantemente apareciendo día a día innovaciones en la materia, lo cual en muchos casos impide que el abogado consulte referencias legislativas relativas al tema, es imperativo que el jurista analice el valor jurídico del documento electrónico y lo tutelé de tal forma que a las personas se les ofrezca seguridad y confianza en los nuevos documentos a la par de permitir una eficaz utilización de las nuevas tecnologías. Para ello, primero hay que analizar la normatividad vigente y después establecer la normatividad óptima para tutelar el doble interés antes señalado.

Asimismo, el constante uso de computadoras y el incremento de nuevas tecnologías nos ha conducido a la tendencia que se incrementa día a día de sustituir el documento en soporte papel con firma manuscrita por el documento electrónico con firma digital; este tema debe ser analizado y legislado a fin de dar confianza y seguridad a los contratantes ante las nuevas formas de contratación.

Numerosos países ante el creciente avance informático han tratado de marcar el camino de sus sociedades hacia la "Revolución Digital", entre ellos se encuentran la denominada

Sociedad de la Información (Information Society) promovida por la Unión Europea, y la Infraestructura Nacional de Información (NII: National Information Infrastructure) que se desarrolló paralelamente en los Estados Unidos de Norteamérica. Ésta última fue implementada el 15 de septiembre 1993, siendo una parte esencial para el documento electrónico al tratar de la infraestructura de firma digital.

Por desgracia, en nuestro país no se ha dado ninguna iniciativa de alcance semejante a las anteriores lo que ha producido que el común de la población desconozca los alcances e implicaciones de la era de la información.

En México no hay suficiente difusión de que son y como operan los medios informáticos para lograr un cambio cultural, el costo de acceso o de adquisición a los mismos es elevado, y existen numerosos problemas técnicos.

Dicho retraso se encuentra también en materia legislativa donde apenas se empieza a incursionar en la materia. Aunque, ese retraso nos brindará la oportunidad de gozar de la experiencia acumulada por otros países, lo que nos permitirá tener un avance concreto al utilizar únicamente lo que les ha resultado eficaz, evitando cometer los mismos errores que ellos; aunque se debe tener siempre en mente que toda investigación en la que se haga referencia a la informática, como es el caso del documento electrónico, y la contratación electrónica, implica un desafío, además de que el estudio debe por naturaleza ser interdisciplinario y necesariamente contendrá aspectos técnicos-informáticos.

En cuanto a los documentos electrónicos que transitan por las redes, y especialmente por Internet es necesario volver a repetir que la legislación que se adopte debe tener como principal característica la de ser compatible con legislaciones de otros países, ya que Internet es una red abierta que extiende sus límites fuera de las fronteras y a distancias indeterminadas.

Siendo importante señalar que hasta el momento, en cuanto a Derecho Informático, en general, los países más avanzados en el aspecto legislativo y académico en América Latina, son Chile y Argentina.

Sin embargo, y a pesar de que se incrementa en forma notable el uso y trascendencia de los soportes electrónicos en la contratación y en los medios de pago; dichos soportes han sido objeto de críticas que en su momento fueron validas pero en la actualidad carecen de bases fundamentadas, así en cuanto al documento electrónico se cuestiona:

Su valor probatorio, debido a que la prueba documental en soporte papel, escrita y firmada hasta el momento ha sido considerada como la prueba por excelencia, implicando el documento electrónico un gran desafío para el Derecho Probatorio al contener numerosas diferencias con el documento tradicional;

La estabilidad de su contenido, ya que la inalterabilidad y el carácter indeleble de los elementos de registro empleados desaparece si pueden ser sobrescritos o borrados;

Su originalidad, al no existir una clara diferencia entre el original y las copias; y

Su autenticidad, al no poder aplicarse al documento electrónico en sentido estricto la firma manuscrita, por lo que el problema se encuentra en la aceptación de la homologación de la firma autógrafa a la firma digital.

Afortunadamente, y como se expondrá en esta investigación, la mayoría de las críticas antes expuestas quedan disipadas con los avances tecnológicos y legales actuales, los cuales nos permiten demostrar la seguridad y confiabilidad de los documentos electrónicos.

3.1. El documento electrónico como documento escrito.

La palabra “documento” proviene del latín *documentum*, “es en sí lo que enseña; que *docet*”¹, y se conceptualiza en lenguaje común como un “diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos...es cualquier cosa que sirve para ilustrar o comprobar algo”.² “El documento es un objeto físico destinado a conservar y transmitir informaciones mediante mensajes en lenguaje natural”.³

Las anteriores definiciones nos permiten reconocer que el documento es un objeto material, perdurable, que comunica, e ilustra sobre hechos y mensajes para su posterior comprobación a través de la escritura o de algún otro medio. Sin embargo, debemos reconocer que como lo señala la primera definición, casi siempre que se piensa en un documento en nuestra mente surge la idea de algo escrito, asimismo, la escritura reviste recalcada importancia para el interés jurídico en cuanto a que se considera el medio documental más reconocido y usado; por ello, en el presente apartado nos vamos a circunscribir a la consideración del documento electrónico como documento escrito.

Aunque la mayor parte de la doctrina considera a los registros informáticos como una “manera” de escribir aún existen autores que critican severamente esta consideración.

La comunicación escrita por esencia se diferencia de la comunicación verbal en cuanto a que esta última no es perdurable, y es difícilmente reiterable ante ausentes.

Mientras que la escritura permite comunicar y comprobar. Proviene del latín *scriptura* siendo la acción y efecto de escribir; por su parte, escribir tiene la raíz latina *scribere* significando comunicar a través de un escrito, o “representar las palabras o las ideas con letras u otros signos trazados en papel u otra superficie, por medio de pluma y tinta o de otro instrumento adecuado a este fin, o por medio de la mecanografía”.⁴ La escritura permite comunicar y comprobar. Concibiendo Ettore Giannantonio a la escritura como la fijación sobre un soporte material de un mensaje destinado a la conservación.⁵

¹ Carmelutti citado por Couture, Eduardo J., “Estudios de Derecho Procesal Civil”. Depalma, Argentina, 1989, pág. 56.

² “Enciclopedia Salvat”. Tomo 4. Salvat editores, España, 1976, pág. 1103.

³ Kemper, Ana María. “XXIV Jornada Notarial Argentina. Tema I. Seguridad jurídica en la contratación por medios electrónicos. Documento electrónico”. Buenos Aires, Argentina, octubre 1996. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

⁴ “Enciclopedia Salvat”. Ob. cit., pág. 1244.

⁵ Giannantonio citado por Kemper, Ana María. Op. cit..

Por lo general, la escritura implica redactar signos alfabéticos o cifras del sistema decimal por medio de una pluma sobre una hoja de papel, pero la escritura es más amplia que su modo normal de manifestación. La jurisprudencia italiana ha considerado que el acto debe ser considerado extendido en forma escrita en diversas hipótesis diferentes a las normales: a) en lo referente a la materia, aun si ha sido extendido en materia distinta del papel, como la piel o la tela y, en general, toda otra materia sobre la cual sea posible imprimir con cualquier medio idóneo signos gráficos; b) en cuanto al medio, aun en el caso de que sea redactado no ya con una pluma, sino con un lápiz, con yeso o carbón, y en tanto no sea exigida la autografía, aun con máquina de escribir, sea ésta normal o con caracteres estenográficos; c) en lo relativo al alfabeto, aun si el documento ha sido redactado con un alfabeto extranjero o con letras de imprenta, con sello o con signos estenográficos; d) por fin, y respecto de la lengua, aun si el documento ha sido redactado en una lengua extranjera, en dialecto, en una lengua muerta o en un código convencional, de modo que sea posible comprender el significado. En otra jurisprudencia y ya respecto a los documentos electrónicos se precisa que se debe considerar escrito aun un documento redactado con un lápiz óptico, que no puede ser leído sino mediante una máquina y un procedimiento apropiados; y que, en modo análogo, se debe considerar documento escrito un documento redactado en un lenguaje convencional aunque secreto.⁶

Por su parte, en cuanto al documento electrónico Ettore Giannantonio⁷ indica que los documentos electrónicos en sentido estricto poseen como característica común el que no pueden ser leídos o conocidos por el hombre, sino como consecuencia de la intervención de máquinas traductoras que hacen perceptibles y comprensibles las señales digitales de que están constituidos. Y los define como los documentos formados por un ordenador o el documento formado por medio del ordenador. En el primer caso, el ordenador conforme a una serie de palabras y en base a un software determina la conclusión que se ha de obtener en el caso concreto (se trata de hipótesis raras por el momento). En el segundo caso, el ordenador documenta una regulación de intereses previamente expresada, se limita a comprobar. Dicha actividad de documentación puede asumir formas diversas: El documento puede ser memorizado en forma digital y almacenado en la memoria central del ordenador o en los periféricos de memoria, ocasionando una distinción en virtud de sus diferentes grados de conservabilidad; por ejemplo, los contenidos en la memoria RAM son de carácter volátil mientras que los de la memoria ROM están destinados a permanecer inalterables en el tiempo. Dentro de los documentos en sentido estricto también se puede distinguir a los construidos para el uso de las terminales de un sistema como las tarjetas magnéticas para acceder a un sistema de ventas o a una cuenta corriente bancaria (tarjetas de plástico con un contenido magnético y un número de código personal). A continuación define a los documentos electrónicos en sentido amplio cuya característica esencial es que, dejando a un lado los microfilm para los cuales rige una disciplina particular, son perceptibles y, en el caso de textos alfanuméricos, legibles directamente por el hombre sin necesidad de intervenciones por parte de máquinas traductoras. Son los formados por el ordenador mediante los propios

⁶ "Informática y Derecho. Aportes de Doctrina Internacional". Director Latmark, Daniel R.. Depalma, reimpresión, Buenos Aires, 1991, Volumen 1, p.p. 111 a 113.

⁷ *Ibidem*, p.p. 94 a 99.

órganos de salida; el documento no está en forma digital pero puede estar constituido por cualquier objeto material formado por una máquina conectada con un elaborador.

Una definición más concreta sería que el documento electrónico en sentido estricto es “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 consiste en mensajes digitalizados que requieren de máquinas traductoras para ser percibidos y comprendidos por el hombre”, y en sentido amplio los documentos electrónicos o informáticos son aquéllos “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”.⁸

En estas definiciones podemos notar que los documentos electrónicos en sentido amplio han sido usados durante décadas por la sociedad al no considerarlos como tales, sino como documentos equiparables a los creados por medio de una máquina de escribir; así estos documentos si bien deben ser considerados como documentos informáticos no requieren una regulación tan rigurosa como la referente a los documentos electrónicos en sentido estricto, y es por ello que casi todos los esfuerzos doctrinales y legislativos a los que haremos referencia al mencionar a los documentos electrónicos o informáticos aluden únicamente a los éstos documentos en sentido estricto, un ejemplo de ello es el Decreto No. 427 (Argentina, Buenos Aires, 16 de abril de 1998) que legisla sobre el documento electrónico considerando como tal a la “Representación digital de actos, hechos o datos jurídicamente relevantes.”⁹ Por lo mismo, una vez señalada la diferencia entre documento electrónico en sentido estricto y documento electrónico en sentido amplio esta investigación se centrará en el primero aunque hará algunas alusiones al segundo las cuales serán debidamente señaladas.

Así, resalta como principal diferencia entre el documento escrito y el documento electrónico la característica de que este último no se encuentra en soporte papel, pero no por ello se le puede negar el carácter de documento al documento digital, asimismo, no se le puede negar el carácter de acto escrito por no ser perceptible y comprensible directamente por el hombre, ya que como lo señala la jurisprudencia italiana un mensaje redactado en lenguaje convencional pero secreto puede ser considerado como escrito, al igual que se considera escrito un documento en lengua extranjera o muerta aunque no podamos comprenderlo directamente.

Como ya quedo precisado, la escritura requiere que se fije información sobre un soporte físico a través de signos convencionales como pueden ser los que forman parte de un

⁸ Herrera Bravo, Rodolfo. “El documento electrónico: algunas vías de aplicación en el Derecho Probatorio Chileno”. REDI: Revista Electrónica de Derecho Informático. Número 7, febrero, 1999. Disponible [Online]: <<http://derecho.org/redi/>>

⁹ Decreto No. 427 del 16 de abril de 1998. Argentina, Buenos Aires. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

lenguaje con el propósito de comunicar, por lo que no hay inconveniente para considerar al documento electrónico, como documento escrito, ya que reúne las mismas características que el documento tradicional aceptadas por la generalidad de la doctrina, y reconocidas en la XXIV Jornada Notarial Argentina (Buenos Aires, octubre de 1996)¹⁰:

Contiene un mensaje (desde un texto alfanumérico hasta un diseño gráfico), está “escrito” en un lenguaje de dígitos binario (bits), gravado sobre un soporte material mueble (que le brindan los dispositivos de memoria auxiliar), se encuentra destinado a durar en el tiempo, no requiere la presencia física del emisor y del receptor con lo que supera las limitaciones temporales y espaciales de la comunicación oral, y con el uso de técnicas apropiadas es inalterable.

3.2. Elaboración del documento electrónico.

En la elaboración del documento electrónico intervienen elementos y sujetos, a saber:

a) Elementos.

Los principales elementos son el hardware y el software, éstos en conjunto forman al ordenador, es decir, forman una máquina capaz de recibir y almacenar electrónicamente información, para procesarla y entregar los resultados de esa evaluación como un mensaje, el cual posteriormente puede ser transmitido; y dicho mensaje puede aparejar efectos que tengan una trascendencia jurídica. Razón por la cual la doctrina jurídica considera al hardware como toda máquina capaz de procesar electrónicamente información cuyos efectos tengan una trascendencia jurídica.

El hardware. “El hardware es el soporte físico del ordenador, esto es, la máquina, definiéndose como el conjunto de elementos del ordenador que son tangibles físicamente”.¹¹ Se constituye por partes mecánicas, electromecánicas y electrónicas, y se encuentra formado por el conjunto de la Unidad Central de Proceso y de los distintos periféricos.

En la Unidad Central de Proceso se realiza todo lo necesario para el procesamiento de la información, siendo los periféricos el conjunto de dispositivos utilizados por la Unidad Central del Proceso, adecuados para asumir la información que se ha de procesar.

Así, la Unidad Central de Proceso (CPU) es el elemento primordial del ordenador, al efectuarse en ella las operaciones relativas al procesamiento de la información. Ésta Unidad se compone de tres partes fundamentales:

- ◆ La Unidad de Control. Su misión es la de coordinar a todos los elementos que intervengan en determinado proceso, cuidando su correcto funcionamiento.

¹⁰ Kemper, Ana María. Ob. cit..

¹¹ “Master Informática”. F&G editores, Madrid, 1992, pág. 60.

- ◆ La Unidad Aritmético-Lógica. Su función es la ejecución de operaciones matemáticas básicas (sumar, restar, multiplicar, dividir) y lógicas (“No” lógico, “Y” Y lógico, “U” O lógico) con las que se procesa toda la información; y
- ◆ La Memoria Central. Ésta almacena la información que se ha de trabajar en un proceso cualquiera. La Memoria Central es volátil y se encuentra físicamente cercana al Procesador Central, siendo éstas sus principales diferencias con la memoria auxiliar. La Memoria Central se subdivide en memoria RAM (Random Access Memory) y memoria ROM (Read Only Memory). La memoria ROM únicamente es de lectura, mientras que la memoria RAM es en la que el ordenador guarda temporalmente información.

Por su parte, los dispositivos periféricos son los que canalizan la entrada y salida de la información de la Unidad Central de Proceso convirtiéndose en los medios a través de los cuales dicha Unidad se comunica con el usuario. Los periféricos se clasifican en de entrada, salida, y entrada/salida.

Los de entrada son los medios a través de los cuales se alimenta a la computadora con información por ejemplo, el teclado, el mouse o ratón, las tabletas digitalizadoras, el lector de disco compacto, el escáner, los reconocedores de voz, y las unidades de disco.

Los periféricos de salida son los medios por medio de los cuales se percibe el resultado del proceso llevado a cabo, como la impresora, el monitor, y las bocinas.

Y dentro de los periféricos de entrada/salida se encuentran los periféricos de almacenamiento o memoria auxiliar.

El hardware funciona conforme a criterios lógicos definidos por el software y por los parámetros de programación utilizados, por lo que el hardware necesita del software para que el ordenador se convierta en algo útil que pueda procesar la información requerida.

El programa o software. Es el componente lógico del ordenador, refiriéndose a los programas en general. En el caso de la elaboración del documento electrónico el software adquiere recalcada importancia; los programas serán los que permitan dar seguridad al documento digital, a través de ellos se ejecutarán las reglas técnicas necesarias para que a un documento electrónico se le reconozcan las características jurídicas de integridad, autenticidad, y no repudio. Por ejemplo, en la producción del documento electrónico su inalterabilidad estará dada por la ejecución de un software que refiriéndose a un documento digital específico implemente códigos, llaves y medidas de seguridad que no permitan la alteración de sus datos.

En el software se diferencian principalmente el sistema operativo y los programas de aplicación. En el sistema operativo se conjugan diversos programas que controlan el funcionamiento básico del ordenador, por lo que para que un ordenador sea práctico en diversas tareas es necesario que cuente con varios programas de aplicación, que le dan al ordenador instrucciones precisas sobre las operaciones a realizar en cuanto a una información determinada.

b) Sujetos.

Los sujetos corresponden a aquéllos a los que la Ley reconoce como autores del documento, por lo que como sujetos se debe tomar a las partes contratantes y no al programador, al ser éste ajeno a la relación contractual. Por lo tanto, dentro de los sujetos encontramos a la persona que utiliza el programa preestablecido en la computadora, y a aquella que ejecuta el ordenador.

Primero, una persona utilizando el programa preestablecido en la computadora, elabora un documento electrónico que contiene un acto jurídico, y después la persona que desea el resultado ejecuta el ordenador y produce en consecuencia la efectivización del documento electrónico para ese acto jurídico.

3.3. Características del documento electrónico.

En el estudio realizado en la presente investigación sobre el documento electrónico como documento escrito, se logró establecer que ambos poseen las mismas características las cuales detallaremos a continuación:

1) Contiene un mensaje que puede ser desde un texto alfanumérico hasta un diseño gráfico.

En este aspecto resulta esencial diferenciar entre el mensaje o representación y el soporte que la contiene, así si bien la información no es inmediatamente percible a menos que se usen máquinas traductoras para tal efecto, no por ello puede negarse su existencia, la cual se demuestra al implementarse las máquinas traductoras necesarias para hacer percible el mensaje almacenado en un soporte informático.

2) Está escrito en un lenguaje de dígitos binario (bits).

En un ordenador los datos son internamente representados a través del sistema binario donde a cada dígito se le llama bit; ocho bits representan un byte, el cual a su vez representa un carácter. En este sistema de numeración los únicos dígitos posibles son el cero y el uno, por lo que todos los caracteres del alfabeto son representados en dicho sistema basándose en el código ASCII (American Standar Code for Information Interchange -Código Americano Estándar para Intercambio de Información-).

Por ello, el lenguaje es uno de las mayores obstáculos que ha tenido que superar el documento digital para ser considerado como un documento tradicional, debido a que las nuevas tecnologías ofrecen un lenguaje técnico no comprensible directamente por el hombre; se necesita de la mediación de una máquina traductora para lograr la aprehensión de la información existiendo una aparente desmaterialización de ésta.

Pero la realidad es que en el caso de las computadoras los bits corresponden al "alfabeto del lenguaje electrónico", y a pesar de que son entidades magnéticas no perceptibles por los sentidos humanos, constituyen una representación material, y si bien en algunos casos su existencia puede ser volátil en otros puede ser fijada de varios

modos pudiendo adquirir incluso permanencia material superior a la del papel. Así, el lenguaje electrónico es un verdadero lenguaje a pesar de que no puede ser percibido y por lo tanto comprendido directamente por el hombre, porque dicho lenguaje electrónico es un medio de comunicación diseñado no sólo para comunicar algo a las máquinas sino también a los seres humanos a través de los periféricos de salida; es un lenguaje creado para que mediante el funcionamiento de la máquina se dé la comunicación entre ésta y no sólo uno sino la mayor cantidad de seres humanos posibles de manera rápida y eficaz. Además, de que todo documento electrónico puede ser comprendido por el hombre siempre que se use la correspondiente máquina traductora para ello.

Por otra parte, en cuanto a lenguaje electrónico se refiere desde hace algún tiempo se ha implementado el TEDI, (Transferencia Electrónica de Datos Informatizados -en inglés EDI: Electronic Data Interchange-)¹² el cual permite reemplazar al documento en soporte papel en las transacciones comerciales a nivel internacional. Al respecto, Estados Unidos y Europa lograron que en 1986, se creara un lenguaje común para la transmisión de datos informatizados en la administración, el comercio y el transporte (TEDIFACT); con lo que el lenguaje técnico y la legislación trabajando en conjunto permiten armonizar y estandarizar documentos comerciales.

3) Gravado sobre un soporte material mueble (memoria auxiliar).

Como ya se mencionó en el punto anterior los ordenadores se componen de una Memoria Central y una memoria auxiliar; la Memoria Central almacena la información con que se ha de trabajar en un proceso cualquiera y es muy diferente a la memoria auxiliar en cuanto que a la primera es volátil, dado que por regla general sólo almacena información mientras el ordenador se encuentra en funcionamiento; además de que el acceso a ella requiere de mucho menor tiempo que el acceso a la memoria auxiliar en virtud de que está constituida por elementos totalmente electrónicos y se encuentra cercana al Procesador Central.

La Memoria Central se subdivide en memoria RAM (Random Access Memory) y memoria ROM (Read Only Memory). La memoria ROM es sólo de lectura al contener datos grabados por el fabricante que son esenciales para que el ordenador comience a trabajar (arranque). Mientras que la memoria RAM es la memoria de acceso aleatorio, en la que el ordenador guarda temporalmente información.

Por su parte, la memoria auxiliar es la memoria externa del ordenador, está compuesta por mecanismos capaces de almacenar gran cantidad de información de manera

¹² EDI se define como "el intercambio de datos en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales...La característica más importante de este tipo de transacciones es que los mensajes intercambiados están normalizados y perfectamente estructurados de forma que pueden ser procesados por las computadoras de los intervinientes en las transacciones. Las transacciones EDI se realizan sin papeles, utilizando para ello las redes de telecomunicación suministradas por los servicios públicos o privados o mediante servicios de Redes de Valor Agregado (VAN)". Devoto, Mauricio; Lynch, Horacio M. "Banca, comercio, moneda electrónica y la firma digital". REDI: Revista Electrónica de Derecho Informático, número 2, septiembre, 1998. Disponible [Online]: <<http://derecho.org/redi/>>

permanente en un objeto material o soporte de almacenamiento masivo, como discos duros, discos flexibles, discos compactos (CD-ROM), discos láser, etcétera. Todos ellos almacenan información transmitida por la Unidad Central de Proceso y permiten el acceso a ella a través de los procedimientos adecuados, pero cada uno es diferente al otro, por ejemplo, los discos duros quedan alojados de forma permanente dentro del ordenador (aunque existen algunos que son removibles); mientras que los discos flexibles (disquetes o *floppy disks*) tienen gran capacidad de almacenamiento, bajo costo, y son portátiles; asimismo, los anteriores son diferentes a la cinta magnética la cual normalmente se usa en su formato de cartucho streamer o cinta de backup (copia de seguridad), son más baratas que los discos magnéticos pero con la problemática de que la información no puede ser consultada de manera selectiva, al sólo poderse leer de principio a fin el archivo almacenado, además de que tienen escasa velocidad de trabajo.

Por lo que, los dispositivos de memoria secundaria son los que nos permitirán darle el soporte material mueble al documento electrónico; en ellos la información se grava como cuando normalmente se usa un soporte en papel, existe lo que podría considerarse como el papel (superficie magnética u óptica) y el equivalente a la pluma (diminuto electroimán o cañón láser). La información contenida en un documento electrónico es almacenada utilizando un soporte magnético u óptico que provoca que se desplace una cabeza de lectura/escritura, compuesta por un diminuto electroimán o cañón láser equivalente, sobre la superficie magnética. Permitiendo que se almacene y recupere información tantas veces se requiera.

Así, si bien no todos los dispositivos de memoria secundaria son muebles el uso de aquéllos que lo sean nos da un perfecto soporte para la información.

4) Inalterable.

La tecnología trastorna el concepto del documento como algo inalterable con la introducción del documento electrónico que permite realizar cualquier cambio de acuerdo a las necesidades de la información. Pero no todos los documentos electrónicos son alterables, sólo lo son aquéllos en los que no se han tomado las respectivas medidas de seguridad a que se hará mención en este apartado.

5) No requiere la presencia física del emisor y del receptor con lo que supera las limitaciones temporales y espaciales e la comunicación oral.

No requiere la presencia física de emisor y receptor debido a que el mensaje transmitido por el emisor se encuentra contenido en un soporte informático, el cual puede ser consultado por el receptor en lugar y tiempo diferentes a aquéllos en los que se almacenó la información, de la misma forma que ocurre con cualquier documento en soporte papel.

6) Ventajas del documento digital.

La utilización de documentos electrónicos acarrea numerosas ventajas, entre ellas se encuentran su alta resolución, con lo que se logra una imagen de alta calidad; su perdurabilidad; su alta capacidad de almacenamiento de información por disco; la posibilidad de que varios usuarios accedan a ellos al mismo tiempo; una

recuperación rápida y efectiva (visualización de la imagen del documento consultado en milésimas de segundo); si se usan medios telemáticos, los documentos digitales son independientes de la distancia que exista entre el lugar físico del archivo y el de la consulta; y se encuentran protegidos ante factores externos que afectan a otros soportes como podrían ser las plagas, los hongos, y el frío.

Sin embargo, es necesario precisar que dada la naturaleza del documento electrónico, para que sea reconocido como documento en sí deberá conjuntar determinada cantidad y calidad de medios técnicos que le permitan poseer seguridad integral; cuando un documento digital es integralmente seguro garantiza la confidencialidad, integridad, autenticación y no repudiación:

El principio de CONFIDENCIALIDAD se relaciona con el Derecho a que ciertos aspectos de nuestra vida permanezcan como privados ante terceros. En México, es el artículo 16 constitucional el que establece que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones sino en virtud de mandamiento escrito de autoridad competente que funde y motive la causa legal del procedimiento; y que las comunicaciones privadas son inviolables, así como la correspondencia cuando se utilice el servicio de correos. Pero en nuestro país, todavía no existe protección eficaz para los datos personales. Esta protección, en general, en Estados Unidos y en diversos países de la Unión Europea, implica la aplicación de penas en caso de que se difundan mensajes que puedan divulgar información que constituya una invasión a la privacidad, además de que se les protege contra el monitoreo electrónico por autoridades gubernamentales y particulares.

El principio de INTEGRIDAD implica que los datos contenidos en un documento electrónico no han sido alterados. En los documentos informáticos hasta el momento la mejor forma de garantizar este principio es añadiendo la firma electrónica; en este caso el principio de integridad implica que los datos no han sido alterados desde el momento en que se agregó la firma electrónica al documento digital.

El principio de AUTENTICIDAD permite tener seguridad de que la firma digital pertenece a la persona que firmó, dando certeza a cada una de las partes de que la otra es efectivamente quien dice ser. Para garantizar este principio electrónicamente se recomienda el uso de protocolos de seguridad como SET y del uso de firmas digitales basadas en una infraestructura de firma electrónica.

El principio de NO REPUDIO se resume en que cuando una persona añade su firma digital está dando su conformidad con el contenido del documento, por lo que las partes no podrán desconocer las obligaciones que emanen del acto jurídico representado en el dicho documento, salvo en los casos establecidos en las leyes.

7) La seguridad integral.

La seguridad en los documentos electrónicos es esencial, asimismo, es indispensable la seguridad en las computadoras que intervienen en su elaboración, ya que una computadora

puede cometer en milésimas de segundo errores tan graves que se hubiera necesitado de cientos de hombres y días enteros para cometer uno igual.

Para dar seguridad tanto al documento electrónico como a los computadoras se necesita de mecanismos y servicios humanos, físicos y tecnológicos que deberán ser usados en conjunto para obtener una seguridad integral.

Para ello la Comisión Europea creó el Libro Verde de la Seguridad de los Sistemas de Información (SSI), el cual plantea el Modelo de Seguridad orientada a la Empresa, que incluye:

Seguridad en sistemas operativos, servicios y protocolos de comunicación, plataformas finales, software, y herramientas de aplicación como el correo electrónico. En ellos, la seguridad y la funcionalidad deben estar equilibradas, pero manteniendo como objetivo asegurar que existan mecanismos apropiados para preservar la integridad de datos, permitiendo incluso la recuperación de un documento después de un fallo -tanto cuando el documento es almacenado como cuando es transmitido entre dos entidades-, asimismo se debe garantizar la comunicación eficaz con entidades alejadas, permitir accesos sin que se revele la identidad del usuario, y que el sello de fecha y hora sea emitido por un ente confiable, ya que de lo contrario será difícil su prueba.

De la misma forma, la evaluación de los productos resulta sumamente importante, en 1990 se publicó el Criterio de Evaluación de Seguridad de la Tecnología Informática (ITSEC: Information Technology Security Evaluation Criteria) con la participación de Alemania, Francia, Los Países Bajos y el Reino Unido. Al precursor de este trabajo se le denominó el "Libro Naranja". Estos proyectos se realizan con el propósito de proteger la información de desastres, entendidos mundialmente como la interrupción en la capacidad de acceso a la información y procesamiento de la misma, necesaria para la operación normal de la empresa.¹³ Las interrupciones pueden ser de naturaleza física, como los terremotos, relativas al personal, organizativas o técnicas. Los proyectos abarcan la prevención de los desastres, la protección contra los mismos, y el desarrollo de las reglas a implementar en caso de que algún desastre ocurra para que la recuperación tome el menor tiempo posible.

Contra las amenazas técnicas se utilizan contramedidas técnicas, que consisten en mecanismos de seguridad del propio sistema, y contra el resto se usan contramedidas no técnicas. En cuanto a las telecomunicaciones se desea que se proporcione un servicio de seguridad como parte del servicio de telecomunicaciones, lo que permitirá que todas las entidades involucradas en la prestación de éste servicio deban adoptar las medidas de seguridad preestablecidas.

En México existen proyectos similares y tradicionalmente se implementan planes de contingencia y de seguridad de la información (en otros países denominados DRP: Disaster Recovery Plan -Plan de Recuperación contra Desastres-). Estos planes son cada vez más utilizados, sobre todo en nuestros días debido a que la

¹³ Rodríguez, Luis Angel. "Seguridad de la información en sistemas de Cómputo". Ventura ediciones, México, 1995, pág. 5.

sociedad cada vez se vuelve más dependiente de la tecnología de la información, especialmente en sectores tan importantes como las telecomunicaciones, la banca, y los servicios públicos; siendo primordial proteger el correcto funcionamiento de dicha tecnología, ya que las consecuencias financieras pueden ser desastrosas si los sistemas fallan, se equivocan, o pierden información.

Por ello, las medidas de seguridad deben considerarse como parte de la inversión total y el tipo de seguridad dependerá de la información que se está protegiendo y de la amplitud del presupuesto que se posea; por desgracia todavía no se toma conciencia de ello, debido a que la seguridad tiene costos tangibles pero beneficios intangibles. Surgiendo dos preguntas esenciales ¿qué información merece especial protección? y ¿cuánto cuesta un minuto sin poder trabajar por un desastre?

El problema de seguridad parte desde los fabricantes, en cuanto a la calidad de los productos, por lo que, respecto a la seguridad de datos se deben proteger las instalaciones físicas, los procedimientos operacionales, el hardware, las redes y comunicaciones, y el software.

Dentro de las prevenciones a adoptar para prevenir desastres se encuentran¹⁴: instalar luces de emergencia y sistemas de comunicación que puedan funcionar con baterías; tener sistemas de rociadores y construir con materiales no inflamables; en cuanto a la seguridad de la información se debe clasificar ésta conforme a su importancia para dar la cantidad de seguridad que necesite cada tipo de información; mediante políticas y procedimientos internos seleccionar y mantener el control del personal; mantener control físico de acceso al centro de cómputo o a secciones del mismo; proteger a los ordenadores y al software manteniendo condiciones óptimas de humedad, temperatura, polvo, etcétera; tener seguridad en las comunicaciones mediante la implementación de encriptación, enrutamiento diverso, y call-back modems, entre otros; implementar seguridad lógica, es decir mantener el acceso controlado a los sistemas de información protegiendo a la información misma; evaluar los riesgos reduciendo la posibilidad de que ocurran y preparándose en caso de desastre; y permitir que sólo personas con los conocimientos necesarios tengan acceso al equipo y a la información protegida, este punto se incluye porque debido a la facilidad relativa de operación de los nuevos programas éstos pueden ser usados por personas con poco conocimiento tecnológico pudiendo causar desastres, primordialmente en las redes a causa de la interconexión.

De igual forma se debe considerar que todo equipo de cómputo emana ondas electromagnéticas y éstas pueden ser recogidas y decodificadas a cientos de metros de distancia; esto se puede mitigar eliminando o degradando las emanaciones con tecnología Tempest que viene en dos formas: productos protegidos contra Tempest y cuartos "aislados".

Para recuperarse exitosamente de un desastre se debe tener un plan de recuperación asegurando la disponibilidad de activos o recursos para la recuperación y reduciendo el impacto del desastre a un nivel aceptable por la empresa. Dicho plan de recuperación incluso debe incluir la posibilidad de traslado físico de la empresa a un nuevo lugar.

¹⁴ Ibidem, p.p. 20 a 60.

En cuanto a las personas físicas se recomienda proteger la terminal cuando no se esté usando (siempre cerrar la sesión para evitar la intromisión de extraños); proteger físicamente los equipos manteniendo comidas, bebidas y artefactos eléctricos en lugares alejados; proteger contraseñas (*password*), claves o cualquier código, manteniéndolos en secreto, para ello se debe evitar escribirlos o guardarlos en lugares de fácil acceso o lógicos; proteger los soportes físicos de la memoria auxiliar (discos, cintas, etcétera) y la información confidencial impresa o altamente restringida, éstos se deberán guardar bajo llave cuando no se estén usando; restringir el acceso a sus datos; proteger especialmente datos considerados como confidenciales contenidos en un soporte físico; protegerse contra desastres siempre teniendo respaldos de sus programas y archivos; destruir los datos considerados como confidenciales cuando ya no los esté usando; poner etiquetas de clasificación en todos los documentos y medios de almacenamiento, pero que dichas etiquetas se escriban en lenguaje secreto o en alguna forma que impida que terceros puedan tener conocimiento de que documentos y medios de almacenamiento contienen información que debe permanecer confidencial; no usar programas "pirata", son inseguros e ilegales; una vez concluido el trabajo no dejar nada sobre el escritorio; no hablar de información confidencial en lugares públicos; al elegir un *password*, la elección deber ser hecha con cuidado, no usando sus iniciales, apodo, nombre de familiares, etcétera, es decir, no use datos asociados con su persona; se aconseja el cambio periódico de las contraseñas, claves o códigos, en especial antes de ausentarse por periodos prolongados o estar trabajando con información confidencial; se debe procurar utilizar sistemas operativos y software que no sea relativamente nuevo en el mercado, la novedad del producto implica que todavía no se tenga suficiente experiencia de los obstáculos que su implementación implique; y se debe cuidar la compatibilidad ente equipos utilizando sólo aquéllos que se sepa que son compatibles, en especial con el equipo usado con otros usuarios a los que se desea mandar información.

Una vez que se ha explicado porque es necesaria la seguridad de los documentos electrónicos a continuación se desarrollarán brevemente algunos de los mecanismos o servicios tecnológicos más usados para lograr esta seguridad en sus diferentes aspectos;¹⁵ pero para lograr la seguridad integral a la que ya se ha hecho mención se necesitarán implementar varios de ellos en forma conjunta:

♦ Calidad del software. Un software sometido a una evaluación de calidad adecuada es libre de virus, libre de errores, y eficiente. Resulta esencial la evaluación de calidad para evitar problemas y vulnerabilidades que en muchos sistemas están ligados a errores y fallas en los diseños. En Estados Unidos y Europa se ha tratado de lograr una uniformidad en cuanto a los criterios de evaluación para que aquéllos que participan en el proceso (en especial los fabricantes) no tengan que realizar evaluaciones de calidad con criterios y esquemas diferentes para un mismo producto, lo cual sin duda aumenta el costo sin aumentar la seguridad. Un resultado de ese esfuerzo son las normas de la serie ISO-9000 que buscan la calidad a través de un enfoque de evaluación y certificación.

¹⁵ El desarrollo de mecanismos o servicio tecnológicos para lograr seguridad abarca sólo los que hasta el momento se reconocen dentro de los de mayor demanda en el mercado y de los que se ha comprobado su eficiencia en campos determinados; por ello muchos se han dejado fuera y algunos más se están creando

- ◆ **Código secreto.** Se reconoce como una combinación de cifras y/o letras tecleadas por una persona haciendo uso de un determinado sistema, por ejemplo, los números de identificación personal.
- ◆ **Controles de paridad y de disparidad.** Son programas en los que a los bit que componen un carácter se agrega un bit suplementario magnetizado si es par (control de paridad; viceversa si la técnica adoptada es la de control de disparidad); el ordenador confronta el bit suplementario con el cálculo de los bit que constituyen la palabra y el carácter con cada transferencia.
- ◆ **Control de paridad/disparidad longitudinal.** En estos programas además del control de paridad/disparidad sobre cada carácter, se efectúa un control ulterior de todos los bit que tienen la misma posición dentro de los caracteres transferidos como un bloque unitario.
- ◆ **Corrección de errores.** Consiste en un software que asegura que los datos usados sean correctos, para ello el sistema corrige los errores manejando la corrección como una transacción separada que es grabada y contabilizada.
- ◆ **Criptografía.** La criptografía implica el desarrollo de sistemas que realicen las funciones del campo de estudio de la criptología a saber: la ocultación, disimulación o cifrado de la información; aunque la criptografía se enfoca únicamente a los datos, texto e imágenes.
- ◆ **Detección y expulsión de intrusos en el sistema.** Son programas que fijan un número determinado de intentos que se pueden hacer para entrar al sistema, una vez agotados el sistema se bloquea automáticamente durante un tiempo determinado.
- ◆ **Discos ópticos.** Se recomienda el uso de los discos ópticos debido a ser un soporte permanente e inalterable, y en especial de los CD-WORM (Write Once Read Many); discos que pueden ser leídos muchas veces pero escritos una sola vez.
- ◆ **Estrategia Penop.** Implica el uso de un lápiz electrónico para lograr la autenticación.
- ◆ **Técnica del doble o triple tecleo.** Está técnica se realiza a través de un programa y con el uso de dos o tres terminales distintas. El programa señalará automáticamente las divergencias entre los varios tecleos.
- ◆ **Programas específicos para la fase de memorización y cargo.** Éstos verifican que los datos memorizados sean formalmente homogéneos con los campos a que son destinados, usando en las redes el criterio de la verificación de mensajes.
- ◆ **Restricciones de tiempo de acceso.** Se pre-establecen ciertos periodos dentro de los cuales el usuario puede tener acceso al sistema, descartando aquéllos en los que no tenga necesidad de ello (por ejemplo: fines de semana) en cuyo caso el sistema niega el acceso automáticamente.
- ◆ **Sellos del software.** Protegen a los programas gracias a que el ordenador asocia a cada instrucción o serie de ellas un valor numérico, si el programa se modifica el valor de todas las instrucciones que lo componen se altera, por lo que el ordenador al verificar una disimilitud entre la clave criptográfica y el valor numérico del programa rechaza la ejecución del mismo y señala la alteración.
- ◆ **Sistema biométrico.** Se basa en que algunas características del individuo no son reproducibles y por lo tanto infalsificables, asimismo, no pueden ser reveladas accidentalmente ni ser perdidas o duplicadas. El control del dato biométrico lo efectúa el ordenador y no el hombre, ya que el primero posee una capacidad de individualización y reconocimiento muy superior a la del segundo, pudiendo usarse perfectamente para la

identificación de una persona. El sistema no permite que los datos biométricos utilizados sean reconstruidos desde otros sistemas; siendo los datos biométricos más usados las huellas digitales, la configuración de los vasos sanguíneos de la retina, la geometría de la mano, las huellas de los labios, el reconocimiento de la voz, y el reconocimiento de la grafía del individuo. En su mayoría se encuentra aún en fase de experimentación, pero se augura que será un mecanismo efectivo de autenticación.

- ◆ Terceras Partes Confiables o Autoridades de Certificación (TTP's: Thrusted Third Parties o CA: Certification Authorities). Una Autoridad de Certificación es un tercero confiable que acredita la identidad de aquél que aparece en un certificado y el nexo entre éste y una determinada clave. Actúan como una especie de Notario Electrónico que extiende un certificado, el cual está firmado digitalmente por él para así garantizar la autenticidad de dicha información. Entre los principales servicios que ofrecen destaca su intervención en las firmas digitales certificando que todos los datos contenidos en un certificado de clave pública (nombre, dirección, y clave pública, entre otros) corresponden a los manifestados por la parte que hace referencia a ellos. Para su establecimiento se requiere que en el país de que se trate existan las bases legales para ello y que estas bases (de preferencia) sean armónicas con las establecidas en otros países para que su actuación sea reconocida en el resto de la comunidad internacional.

Estas autoridades también puede actuar como autoridades de fechado digital (TSA: Time Stamping Authorities), en cuyo caso, vinculan un instante de tiempo y en ocasiones de lugar a un documento electrónico, avalando con su firma digital la existencia del documento en el instante (y, en su caso en el lugar) referenciado.

Las Terceras Partes Confiables incluso fueron recomendadas por la OCDE (Organización para la Cooperación y Desarrollo Económicos) para la identificación de las partes contratantes.

- ◆ Tiempo de espera en la Terminal (Terminal Timeout). Si después de un tiempo predeterminado no se registra ninguna actividad en la terminal o estación de trabajo se cierra la sesión automáticamente.

- ◆ Vault Registry o certificado digital de la IBM. Se trata de garantizar las transacciones electrónicas con tecnología de identificación de los usuarios que realicen operaciones e-business.

En el caso de documentos electrónicos transmitidos por medios telemáticos, como son las redes, reglas especiales de seguridad deben ser aplicadas debido a que las redes son en principio un medio inseguro al ser computadoras interconectadas; la inseguridad deriva de su naturaleza multiusuario, de los multirecursos y de los multisistemas, situaciones que incluso pueden acarrear problemas de incompatibilidad con los equipos que van a recibir la información, pero su punto vulnerable por excelencia es que cada nodo no está preparado para un uso compartido de usuarios sobre los que tiene un control limitado o nulo.

En el caso de Internet los principales riesgos son en cuanto a la confidencialidad, y al monitoreo de acceso, sobre todo en casos concretos como el de transmisión de información financiera o datos protegidos por secreto profesional. Internet, en general, carece de seguridad debido a ser una red abierta la pública y al uso de protocolos no protegidos.

Así, para transmitir información por medios telemáticos primero debemos confirmar que las computadoras a utilizar (la del receptor, la del emisor, y de ser posible las de los intermediarios) son seguras, para después podernos centrar en el aspecto más vulnerable que es la red en sí; para su protección existen mecanismos y servicios como los anteriormente enumerados y además los siguientes:

- ◆ Call Back Systems. Son sistemas de control de acceso remoto al sistema (a través de módem). Una vez recibido y aceptado un código (clave, contraseña, etcétera) determinado el módem cuelga y llama al teléfono registrado como el del lugar donde se encuentra la terminal que tiene derecho a entrar en ese sistema.
- ◆ Dispositivos de protección de puertos (PPD). Estos dispositivos incluyen microprocesadores con lógica programada que se colocan en un circuito para evitar el acceso no autorizado. Los microprocesadores tienen la capacidad de registrar peticiones de entrada, checar *passwords*, números de identificación u otros códigos, antes de permitir el acceso a la computadora anfitriona.
- ◆ Enrutamiento diverso. Se envían los mensajes separados en partes y/o por diversos medios.
- ◆ Formato de documento portátil (PDF). Previene la modificación de un documento una vez gravado.
- ◆ Canales seguros de comunicación. Son canales o protocolos que a su vez agrupan un conjunto de protocolos garantizando la confidencialidad y la integridad de las comunicaciones, como:

⇒ Secure HyperText Transfer Protocol (SHTTP) que justamente se aplica a las conexiones HTTP.

⇒ Secure Socket Layer (SSL de Netscape) y el Protocolo de Microsoft (PCT). El primero es de los más utilizados al ser una eficaz forma de encriptar los números de tarjetas de crédito y datos bancarios, su función es la de certificar digitalmente la identidad del vendedor más no la de los compradores. Ambos encriptan las sesiones de comunicaciones y otorgan autenticación del servidor, siendo más versátil el correspondiente a Microsoft al tener compatibilidad con varios protocolos. Pero al no brindar seguridad integral deben conjugarse con el Protocolo SET.

Sistema o Protocolo de Transacciones Electrónicas Seguras (SET: Secure Electronic Transaction). Este protocolo se dice que es la solución a la falta de seguridad para realizar transacciones y pagos a través de Internet, al ser un sistema de criptografía desarrollado por Visa y Mastercard International para operar o realizar pagos en redes abiertas. Utiliza tanto el sistema de criptografía asimétrica como el de criptografía simétrica, gracias a lo cual evita la lentitud del sistema asimétrico y da una garantía de confidencialidad, autenticidad, integridad y no repudio del mensaje. Este sistema funciona con la base de que todos los mensajes se firmaran digitalmente y los intervinientes deberán estar certificados electrónicamente; para ello los bancos emisores y las entidades administradoras de tarjetas de crédito certifican las firmas digitales, y se aseguran de la identidad de los titulares de las tarjetas, asimismo, certifican a los establecimientos comerciales afiliados al sistema, respectivamente. Sin embargo, es un tercero autorizado quien proporciona los certificados digitales a los bancos emisores y

empresas administradoras de las tarjetas de crédito, quienes a su vez los otorgan a los tarjetahabientes y a los establecimientos comerciales, todo ello operado a través de un software denominado "billettera electrónica". El sistema opera de forma virtual sin requerir contacto físico entre el tarjetahabiente y comercio, y aumenta la confidencialidad al impedirse que el establecimiento comercial tenga acceso a los datos bancarios del cliente.

♦ Otras medidas de seguridad en redes son conocer y revisar periódicamente los conductos, enlaces y cables respectivos de las comunicaciones, pero nunca etiquetarlos porque ello podría dar a conocer su función a extraños; sólo computadoras seguras deben estar conectadas a la red, ya que una sola da el acceso para penetrar a la red entera; para reducir las interferencias y emanaciones se debe usar fibra óptica siempre que sea posible; al transmitir información se puede ocultar la información de interés con información "basura"; deben utilizarse las rutas más seguras para transmitir información; un enlace de comunicaciones fijo puede ser probado con un dispositivo especial que lea la firma del enlace para producir un espectro de señal único con lo que cualquier interferencia con el enlace cambiará su firma; se debe ser cuidadoso con lo que se transmite; y tener cuidado con los archivos temporales que crean muchas aplicaciones, dichos archivos deben reenrutarse a un soporte de memoria auxiliar para mejor control.

Día a día aparecen nuevos sistemas y sólo el tiempo podrá decir si son seguros; nuestro país tenía la desventaja de que la tecnología nos llegaba atrasada con respecto a países de primer mundo (en algunos casos este criterio todavía se aplica), sin embargo, en la actualidad las nuevas tecnologías son aprovechadas y difundidas ampliamente por empresas de software y hardware.

Una vez planteados los mecanismos y servicios para lograr una seguridad integral es necesario recordar, que en lo referente a documentos electrónicos al igual que tratándose de cualquier otro documento, nunca se podrá tener una situación totalmente controlada; siempre existirán riesgos ya que ninguna medida de protección es totalmente infalible, pero, el implemento de éstas minimizan notablemente los riesgos y nos permiten implementar documentos electrónicos seguros. Debemos tomar conciencia de que el uso de tecnología implica la necesidad de tomar cuanta precaución sea posible para evitar consecuencias desastrosas, y que la inversión de tiempo y dinero deberá ser directamente proporcional al valor de la información.

3.3.1. Criptografía.

La criptografía o arte de inventar cifras se usa desde tiempos de Julio César, brinda un alto grado de seguridad al permitir la codificación de todo el contenido del documento incluyendo a los elementos de autenticación.

En forma general se divide en cifradores de sustitución y cifradores de transposición. En los primeros cada letra o grupo de ellas se sustituye por otra letra o grupo de letras para disfrazarlas preservando el orden preestablecido; existiendo varios tipos de sustitución, entre ellos la sustitución monoalfabética que sustituye letras, la sustitución

poligramática que sustituyen grupos de letras, y los sistemas tomográficos que sustituyen fracciones de letras. Por su parte, los cifradores de transposición reordenan las letras sin disfrazarlas.

La criptografía es una técnica basada en un algoritmo matemático que encripta o transforma la información legible (texto plano o texto claro) en una ilegible (texto cifrado o cripto) según un procedimiento y usando una clave determinada, hasta que se le aplique el mismo procedimiento y una clave secreta para desencriptarlo o descifrarlo. Como desventajas del uso de criptografía se encuentran que casi siempre implica la reducción de la velocidad de operación del sistema, y que se deba proteger la clave utilizada; pero como ventajas se hallan su costo razonable y alto nivel de seguridad.

La criptografía es muy antigua pero se le había utilizado con respecto a información diplomática o sobre todo en relación con información militar. Es hasta nuestros días cuando se pone disponible al público para dar seguridad y confidencialidad a las transacciones, principalmente, a las que son realizadas en redes, siendo en este aspecto su uso más generalizado el de creación de firmas digitales, por lo que se le reconoce hasta el momento como el mecanismo más eficaz para la protección de documentos electrónicos.

Existen principalmente dos clases de criptografía utilizadas en las firmas digitales:

* La criptografía simétrica o sistemas de criptografía de clave privada o de clave secreta, como Data Encryption Standar (DES) de la IBM, que fue reconocido el 15 de julio de 1975 por el National Bureau of Standars (La Agencia Nacional de Estándares) como el estándar a usarse en los Estados Unidos. Este sistema maneja una sola clave privada que es conocida tanto por el transmisor como por el receptor del mensaje, por lo que con la misma clave se encripta y desencripta el mensaje.

El uso de una sola clave es muy impráctico debido a que en caso de recibir mensajes de varias personas se tiene que poseer una clave privada diferente para desencriptar cada mensaje recibido; e insegura, ya que la clave privada debe ser comunicada a la parte que va a recibir el mensaje incrementándose las posibilidades de que se haga de conocimiento de un tercero o se pierda, además cuando dos personas usan la misma clave siempre existe la posibilidad de que una olvide firmar electrónicamente con lo que no se logrará una autenticación efectiva al no poderse saber cuál de las dos firmó y cuál no lo hizo.

* La criptografía asimétrica o de clave pública surgió en 1977 y fue denominada RSA (siglas que conmemoran a sus inventores Rivest, Shamir y Adleman). En ella se utilizan dos claves, una pública que es de conocimiento general -usualmente se hace de conocimiento a través de su publicación en un directorio electrónico o *white pages* al que cualquier persona puede tener acceso- y otra privada que sólo conoce su poseedor, siendo ésta última la que se usa para "firmar" el documento electrónico permitiendo su autenticación. Debido a que la clave pública correspondiente sólo puede desencriptar mensajes encriptados con una determinada clave privada, no puede el usuario desconocer que es el autor del mensaje.

La criptografía asimétrica es mucho más práctica que la simétrica, ya que cada usuario usa únicamente su par de claves para encriptar todos mensajes que envíen y para desencriptar todos los que reciba. Además, de que brinda mayor seguridad al usuario de la clave pública, al ser el único que conoce su clave privada.

Tratándose de sistemas de criptografía asimétrica a partir de 1991 el software utilizado por personas privadas fue el denominado Pretty Good Privacy (PGP) creado por Phil Zimmermann. Dicho software ha tenido gran aceptación al considerarse virtualmente inexpugnable y se ha distribuido de forma gratuita en Internet.

Sin embargo, existen algunos problemas que pueden presentarse con el uso de la criptografía asimétrica, a saber:

- Los algoritmos de encriptación asimétrica son 100 veces más lentos que los algoritmos de encriptación simétrica.

- Un problema que ya está adquiriendo importancia en los Estados Unidos es que no se pueden confiar en que una persona velará diligentemente para proteger su clave privada, las claves pueden ser perdidas, olvidadas o robadas, tornando inútiles los datos encriptados. Para evitarlo se aconseja el cambio de clave cuando sea necesario o incorporar la clave en un medio físico tal como un chip o una tarjeta magnética (para lo que se tendrá que contar con un lector especial). Probablemente la mejor solución sea pertenecer a la infraestructura de la firma digital la cual permite que en caso de que la seguridad de la clave privada sea comprometida por cualquier motivo, ésta y el certificado que la avala sean inmediatamente revocados.

- Al ser la clave pública de conocimiento general diversas personas pueden encriptar mensajes utilizándola. En realidad éste difícilmente puede considerarse un problema, ya que los mensajes sólo pueden ser desencriptados con la clave privada correspondiente.

- Al no ser la clave pública de conocimiento restringido, es complicado saber si ésta efectivamente pertenece a su titular. Esta dificultad se resuelve en varias legislaciones con la implementación de terceras partes ajenas a las transacciones, las cuales emiten y resguardan las claves públicas garantizando su autenticidad.

- Asimismo, una persona puede crear un par de llaves falsas y diseminar la pública como si fuera de otro persona, lo cual se evita con el uso de Pretty Good Privacy y con los certificados de clave pública de la infraestructura de firma digital.

3.3.1.1. Funcionamiento de la criptografía.

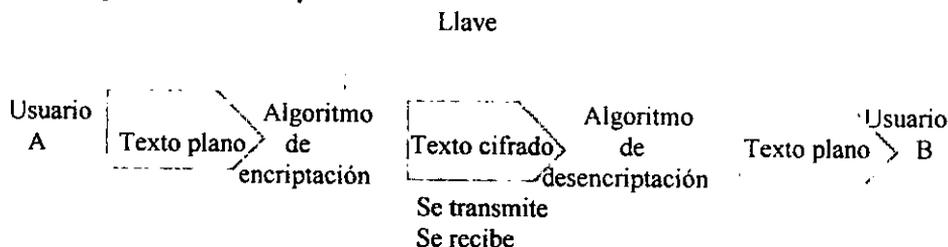
En cuanto a ambos sistemas de criptografía se recomienda que si bien alguna clave debe permanecer secreta, es conveniente que el algoritmo de transformación sea público y estándar por motivo de compatibilidad de equipos entre diferentes fabricantes. Asimismo, comienza a reconocerse que el mejor sistema criptográfico es el que combina la rapidez del sistema simétrico y la seguridad del sistema asimétrico.

En ambos sistemas el proceso de encriptación consiste en un algoritmo y una llave o clave (cadena de bits relativamente corta) que controla el algoritmo. El algoritmo producirá

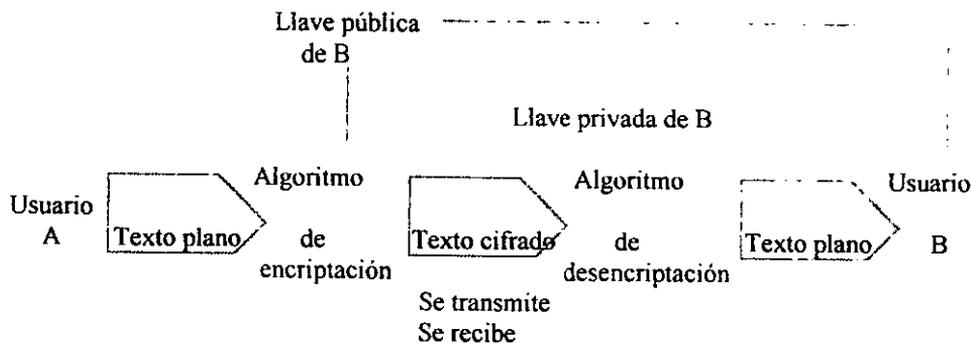
una salida diferente dependiendo de la llave utilizada, por lo que si se cambia la llave se afecta dramáticamente la salida del algoritmo. Y funciona de la siguiente forma:

- 1) Se redacta el mensaje que se desea transmitir (texto plano);
- 2) Se aplica el algoritmo de encriptación por medio de una llave;
- 3) De la operación anterior resulta un texto cifrado aparentemente sin sentido, ininteligible;
- 4) Se transmite el texto cifrado;
- 5) Se recibe el texto cifrado;
- 6) Con la misma u otra llave (en el caso de los sistemas de encriptación de llave pública) se desencadena el algoritmo de descryptación;
- 7) El resultado de la operación anterior es el texto plano, tal como se originó.

a) Encriptación con llave privada.¹⁶



b) Encriptación de llave pública.¹⁷



En el caso del sistema asimétrico, además de estos algoritmos de encriptación existen otros algoritmos de compresión necesarios para conseguir que la firma digital tenga los mismos efectos que la manuscrita. Se trata de los algoritmos hash (algoritmos de compresión, destilación, de huella digital o de función resumen) que se aplican por medio del software del firmante sobre un determinado texto creando un resumen del mismo denominado hash result o hash value. Son algoritmos matemáticos unidireccionales o que

¹⁶ Rodríguez, Luis Angel. Ob. cit., pág. 113.

¹⁷ Idem.

aplican funciones de no retorno, es decir, lo encriptado no se puede descryptar, obteniéndose un extracto de longitud fija (entre 128 y 160 bits) absolutamente específico para ese mensaje, lo que representa la integridad del documento digital, ya que un mínimo cambio en el mensaje (de un bit) ocasionaría que el resultado obtenido al volver a aplicar la función hash fuera totalmente diferente, produciría un extracto completamente diferente, y por tanto no correspondería con el que originalmente firmó el autor; además de que las probabilidades para que dos textos distintos tuviesen el mismo hash son nulas. Una vez realizado esto se somete a un cifrado mediante la clave secreta del autor.

Así, el funcionamiento de los algoritmos de comprensión es:

- 1) Se crea un texto a firmar;
- 2) El software del firmante aplica un algoritmo hash sobre el texto;
- 3) Se obtiene un extracto de longitud fija específico y único para ese mensaje;
- 4) El extracto se somete al cifrado mediante la clave secreta que será hecho al final del documento;
- 5) Se obtiene un extracto final cifrado con la clave secreta del firmante que permite la verificación de la autoría e integridad del documento firmado digitalmente, por la persona que disponga de la clave pública del autor;
- 6) Para comprobar que la firma realizada es efectivamente válida se necesita la clave pública del firmante (obtenida a través de una autoridad de certificación);
- 7) Se introduce en el software del receptor la clave pública del remitente;
- 8) Se descifra el extracto cifrado del firmante;
- 9) Se calcula el extracto hash que corresponde al texto del mensaje;
- 10) Si coincide el hash calculado con el extracto anteriormente descifrado se considera válida la firma, en caso contrario se tiene un mensaje alterado no válido. La autenticación de las partes se logra a través de este sistema auxiliado por la autoridad de certificación.

3.3.1.2. Exportación de la criptografía.

Desgraciadamente la criptografía es un arma de dos filos; por una parte da garantía de seguridad y confidencialidad en los documentos electrónicos, y por otra disminuye la capacidad de vigilancia de los organismos gubernamentales de procuración de justicia, al permitir la transmisión indiscriminada de mensajes con contenido terrorista o de la temida pornografía infantil, entre muchos otros.

Lo anterior aunado al éxito de Pretty Good Privacy llevó a que en abril de 1993 en Estados Unidos se comenzara a implementar el proyecto llamado "encriptación en custodia" (EES, Clipper o Clipper chip) el cual en febrero de 1994 fue considerado por el Departamento de Comercio como una norma de criptografía federal para información no clasificada e incluso llegó a considerarse como norma nacional; por lo que se teme que en un futuro se convierta en la única técnica de criptografía legal.

La "encriptación es custodia" se basa en un algoritmo simétrico clasificado que se coloca en todo hardware de comunicación (faxes, teléfonos, modems, etcétera); la clave instalada se divide en dos partes una custodiada por el Instituto Nacional de Estándares y Tecnología (NIST: National Institute of Standards and Technology) y la otra por el Departamento del Tesoro -ambas agencias gubernamentales-. Esto permite que en caso de que se requiriera descryptar cualquier información encriptada con Clipper, bastará con que una agencia de procuración de justicia extienda la autorización correspondiente para que tanto el Instituto Nacional de Estándares y Tecnología como el Departamento del Tesoro entreguen la mitad respectiva de cada clave para que dicha agencia pueda descryptar cualquier mensaje codificado con Clipper.

La tarea de desarrollar este algoritmo simétrico clasificado se le encomendó a la Agencia de Seguridad Nacional (NSA: National Security Agency), debido a que esta Agencia fue creada por orden del Presidente Truman en 1952, encargándosele como función principal la de intervención en el área de comunicaciones; interceptando y descifrando las comunicaciones de otros países. Dicha función la ha posibilitado para interceptar la mayor parte -sino casi todos- los mensajes electrónicos que entran y salen de este país, y ha gozado de un monopolio virtual en el área de la tecnología criptográfica, mediante la supresión de toda iniciativa privada no gubernamental en este sector alegando que esta tecnología debe ser celosamente protegida.

Así, y por razones que resultan obvias el pueblo estadounidense se ha promulgado en contra de la "encriptación en custodia" al considerarla como un control indebido y excesivo del gobierno de los Estados Unidos para la transmisión de la información.

Representantes de la industria han alegado que las restricciones impuestas por la NSA impiden la innovación en un área fundamental para la industria de la computación, y provocan que compañías norteamericanas pierdan mercados en manos de competidores de otros países. Sin embargo, el argumento con mayor peso ha sido que el gobierno no puede continuar con el monopolio en tecnología criptográfica, debido a que ya no resulta aceptable la aseveración de que la única información que merece seguridad es la información gubernamental.

Debe crearse una nueva infraestructura donde industria y gobierno trabajen de forma conjunta para ofrecer tanto seguridad nacional como seguridad pública, posibilitando el desarrollo de productos que incorporen elementos de criptografía. En esta infraestructura la industria desarrollará los productos mientras que el gobierno establecerá los estándares a los que se deberá sujetar la primera.

Por su parte, los Estados miembros de la Unión Europea reconociendo los peligros que implica el uso de la criptografía han optado por la implementación de las denominadas terceras partes confiables, las cuales custodiarán las claves privadas de los usuarios y sólo las harán del conocimiento de las autoridades de procuración de justicia cuando medie autorización de juez competente realizada sobre la base de la sospecha de que el contenido del mensaje es de naturaleza delictiva.

Por las mismas razones en Estados Unidos y Canadá en forma genérica se autoriza el uso de criptografía, pero por razones de seguridad nacional, la exportación del software de criptografía está sujeta a regulación e incluso se le incluye en la Lista de Municiones de Estados Unidos dentro de las Regulaciones Internacionales de Tráfico de Armamento (ITAR).

Así, la exportación de software de criptografía, información técnica sobre criptografía o información encriptada puede ser ilegal al considerarse como arma, excepto cuando lo autorice el Departamento de Defensa de Estados Unidos.

En el mismo orden de ideas, en Estados Unidos en 1991 se estableció el Algoritmo de Firma Digital (DSA: Digital Signature Algorithm) como estándar oficial de firma digital; se pretendió que dicho estándar fuera adoptado también por la Unión Económica Europea, la que en un principio accedió, pero posteriormente cuando se le concedió licencia exclusiva a la empresa Public Key Partners (PKP) para el desarrollo de DSA la Unión Económica Europea prefirió adoptar el RSA (sistema de criptografía asimétrica), que ya estaba disponible en muchos productos comerciales, mientras que la DSA tenía un mercado muy limitado.

Sin embargo, en la actualidad con el uso corriente del Internet dichas legislaciones han tenido que ser más tolerantes, por ejemplo, Estados Unidos que en un principio sólo permitía la exportación de productos criptográficos que hicieran uso de claves de menos de 56 bits, pero recientemente permitió la exportación de productos con uso de claves de más de 56 bits siempre que exista un sistema de recuperación de claves o depósito de claves (key scrow).

Pero siendo la criptografía una tecnología tan poderosa en el caso de usarla siempre es necesario verificar su legalidad desde el país del que se emite hasta el país que va a recibir, ya que en su mayoría la legalidad de la exportación depende del tipo de criptografía utilizada y de la persona a la que va dirigida, por lo que, por lo general se autoriza el uso de criptografía de bajo o medio nivel como PGP, pero no de alto nivel o software de criptografía perfeccionado; ejemplo de ello son las legislaciones de la mayoría de los Estados miembros de la Unión Europea, cuyas legislaciones también asimilan las técnicas de criptografía a armamentos.

Actualmente, diversos países se encuentran tratando de legislar al respecto; una propuesta ha sido la de que se requiera de licencia o declaración de uso de software criptográfico para autorizar el mismo. En dicha licencia se especificarán los usuarios del equipo o categorías de usuarios y el propósito de uso, no teniéndose que solicitar nueva autorización sino hasta que se cambie de usuario.

3.4. El documento electrónico como documento jurídico.

Como ya se hizo mención en la mayoría de las actividades del hombre se hace uso de alguna manifestación de la tecnología, principalmente computadoras y medios telemáticos

llegando su implementación a despachos de abogados y Notarías, hasta convertirse en casi imprescindible.

El avance tecnológico ha permitido la realización de contratos electrónicos relacionados con tareas cotidianas, conectándose las partes a través de medios telemáticos como es el caso de las redes; incluso las oficinas públicas cada vez con mayor naturalidad usan soportes magnéticos para recibir y almacenar información, de lo que se ha derivado la creación de sistemas que a futuro permitirán la comunicación vía telemática entre abogados, Notarios, y las principales oficinas públicas y privadas. Dentro de todas estas transformaciones ocasionadas por un fenómeno informático de carácter irreversible, el documento electrónico se proclama como el nuevo soporte de la información, como ya ha quedado reconocido en el Anteproyecto de Ley de Documento e Instrumento Digital de Argentina.¹⁸

Lo antes mencionado es una demostración de porque el jurista debe tomar un rol activo dentro del desarrollo tecnológico, para “repensar” los conceptos tradicionales del Derecho, los cuales si bien continúan vigentes, deberán ser ampliados ante la “Revolución Digital” y sus repercusiones. Así, por ejemplo, en el caso de las nuevas formas de contratar, si bien éstas no afectan el derecho en sí, si implican el uso de un nuevo soporte diferente al papel y se acelera su ejercicio gracias a las ventajas tecnológicas que hacen ello posible.

Numerosos países ya han formado grupos de trabajo conformados por juristas y especialistas en informática para proyectar la legislación que regule al documento electrónico, entre ellos se encuentra Alemania que presentó en el XXI Congreso Internacional del Notariado Latino (Berlín, 1995) un Proyecto Piloto para el Intercambio de Datos entre Notarios y Oficinas del Registro de la Propiedad, y para estudiar la posibilidad de modificación del Código Civil en cuanto a la forma de contratar, y a la Ley de Procedimientos en lo referente a los documentos electrónicos como medio de prueba.¹⁹

De la misma manera, en la XXIV Jornada Notarial Argentina (Buenos Aires, octubre 1996)²⁰ y en el III Congreso Notarial del Mercosur (Uruguay, marzo 1997)²¹ se concluyó que al documento electrónico se le pueden aplicar todos los institutos del Derecho positivo vigente para juzgar respecto de su validez, eficacia y valor probatorio; que el documento electrónico es válido y eficaz como forma de contratación, tanto entre presentes como a distancia; que el valor probatorio del documento electrónico estará dado por la naturaleza del contenido del acto con independencia del soporte utilizado; que el Notariado Latino, reúne las condiciones para otorgar seguridad jurídica a la contratación por medios electrónicos en el marco de la autonomía de la voluntad utilizada por las partes para este fin; y que a fin de evitar lagunas interpretativas que se puedan producir al valorar

¹⁸ Kemper, Ana María. Ob. cit..

¹⁹ Idem.

²⁰ XXIV Jornada Notarial Argentina, Buenos Aires, octubre de 1996. “Tema I. Seguridad Jurídica en la contratación por medios electrónicos. Documento electrónico -considerando-”. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

²¹ Devoto, Mauricio; Lynch, Horacio. Ob. cit..

judicialmente al nuevo soporte documental se propicia la promulgación de una ley específica que recepte los principios y fundamentos expuestos.

Diversos esfuerzos como los antes mencionados se han dado alrededor del mundo, concluyendo en favor de la equiparación del documento digital con el documento jurídico tradicional, permitiendo que al documento informático se le otorgue valor jurídico siempre que se respalde en métodos técnicos y un sistema que asegure la originalidad, la autenticidad, la integridad, y la confidencialidad. Y se convoca a aquellos países que aún no han legislado sobre el tema a promulgar las leyes respectivas tomando como base lo logrado en otros países para armonizar legislaciones; lo cual será un requisito indispensable para el correcto desarrollo del comercio electrónico, de las comunicaciones telemáticas y de las relaciones contractuales entre ellos dado su carácter internacional. Este punto debe tener consideración especial en nuestro país ya que el TLCAN ha provocado el encuentro entre dos sistemas jurídicos diferentes, el common law y la tradición jurídica civilista, además de que se ha incrementado lo que se podría denominar como la circulación transfronteriza de resoluciones extranjeras, es decir, que con el tiempo se volverá común el que a tribunales mexicanos se les solicite el reconocimiento y ejecución de resoluciones extranjeras y viceversa.

3.4.1. El documento jurídico digital.

A consideración de Briseño Sierra²² dentro de los denominados medios de acreditamiento se encuentran los documentos, los instrumentos, los monumentos y los registros. Siendo la principal diferencia entre el documento y los demás medios de acreditamiento antes mencionados su carácter escritural, motivado históricamente en razón de que el documento nace cuando aparece la escritura. De ello se deriva que inicialmente el documento se pueda definir como un objeto material que en forma escritural mediante el lenguaje representa ideas, conceptos y palabras, sobre soportes diversos de los cuales el más usado es el papel.

Tomando como base los datos antes mencionados Cipriano Gómez Lara²³ menciona que si bien existen diversas formas de lenguaje propiamente gráfico expresado por medio de dibujos o de otra clase de signos, éstos no son documentos sino registros o instrumentos, como la multitud de nuevos registros tales como el moderno videotape.

Sin embargo, y como acertadamente José Ovalle Favela señala, en un inicio se consideraba como documento únicamente a lo escrito (concepción estructural), pero dicha noción evolucionó hacia la conceptualización del documento de acuerdo a su función (concepción documental). Así, documento "es una cosa representativa, o sea capaz de representar un hecho",²⁴ es la "representación material idónea para poner de manifiesto la

²² Briseño Sierrado citado por Gómez Lara, Cipriano. "Derecho Procesal Civil". Harla, quinta edición, México, 1994, pág. 141.

²³ Gómez Lara, Cipriano. Ob. cit., pág. 142.

²⁴ Carnelutti, Francesco. "La prueba civil. Cómo nace el derecho. Cómo se hace un proceso". Tribunal Supremo de Justicia del D.F., México, 1993, p.p. 84 y 85.

existencia de un hecho o acto jurídico..., susceptible de servir en caso necesario, como elemento probatorio".²⁵

En forma de resumen Roauanet Moscardó define al documento como un "objeto normalmente escrito, en el que se plasma algo mediante letras u otros signos trazados o impresos sobre el papel u otra superficie, pero que excepcionalmente puede no ser escrito y es un objeto en el que puede representarse un hecho natural, o un acuerdo de voluntad...o ser el resultado de una actividad o de un procedimiento".²⁶

Por su parte, Carnelutti tampoco suscribe la noción de documento a lo escrito y añade que no existen documentos naturales, en virtud de que el documento es un objeto que opera sobre un hecho presente y se proyecta al futuro, cuya fuente (medio de exteriorización) es la actividad del hombre encaminada a crear un aparato exterior para conservar en la memoria el hecho; el documento es un objeto capaz de representar, por lo que esta actividad constituye un momento precedente al documento pero no lo que se representa en él. Así, "el hombre obra en presencia del hecho a representar para componer un aparato exterior capaz de producir el efecto representativo".²⁷

En este orden de ideas, el documento para ser tal debe contener la representación de un hecho o acto jurídico, dicha representación podrá o no ser una manifestación del pensamiento (del saber o del querer), porque de conformidad con Carnelutti²⁸ existen técnicas por medio de las cuales se puede fijar hechos en un objeto exterior sin necesidad de que éstos pasen por la psique humana; sin que se manifieste el pensamiento como es el caso de la fotografía. Por lo que, el objeto de la representación documental puede ser cualquier hecho, lográndose la representación mediante la fijación en un objeto exterior de la manifestación del pensamiento. Esta fijación se obtiene a través de una modificación de los objetos exteriores (papel o en este caso cinta o disco magnético u óptico) para determinar por sí solos o cuando se las somete a determinados procesamientos en quien las percibe, la idea manifestada. Surgiendo un documento como fuente de prueba, como hecho exterior que sirve para que el juez deduzca el hecho a probar.

Así, queda afirmado que la finalidad del documento es perpetuar hechos pasados, ya que por desgracia no se puede confiar este trabajo a la mente humana, que es falible y perecedera. El conocimiento debe plasmarse en papel o en otro soporte perdurable, debido a que de no perdurar el documento sería inútil para conservar por sí la representación de un hecho, surgiendo como los principales requisitos propios del documento la inmediatidad, la permanencia, y la exteriorización física de hechos y/o relaciones jurídicas, lo que permite el conocimiento de terceros del contenido de los actos aunque no se hallan encontrado en el momento de su realización, y un medio de prueba.

²⁵ Pina, de Rafael; Pina Vara, de Rafael. "Diccionario de Derecho". Porrúa, vigesimoprimera edición, México, 1995, pág. 255.

²⁶ Kemper, Ana María. Ob. cit.

²⁷ Carnelutti, Francesco. Ob. cit., p.p. 64 a 109.

²⁸ Ibidem, pág. 103.

De las anteriores definiciones y consideraciones se deduce que el documento jurídico al igual que el documento común es un objeto físico perdurable, un bien mueble, puede ser escrito o no, garantiza que el documento representativo se encuentre disponible para ser consultado por terceros o por los interesados por un tiempo mucho mayor al que lo retendría la mente humana (garantiza la fidelidad) y preserva su contenido permitiendo su posterior prueba; pero además de las características anteriores adquiere otras importantes que son que debe ser legal, representa un hecho (o acto jurídico), y garantiza la inmediatividad considerada por Carnelutti como el desplazamiento de la formación del hecho representativo a un momento precedente al proceso, lo que la sustrae a todas las influencias corruptoras que los intereses en conflicto dentro del proceso puedan ejercitar.

Por ello, Davara Rodríguez afirma que “el llamado documento electrónico se encuentra enmarcado en la gran clase de los documentos en el más estricto sentido jurídico y que, como tal, tendrá la misma consideración y validez que cualesquiera otro de los documentos tradicionalmente aceptados”.²⁹

3.4.1.1. Documentos materiales y literales.

Se reconoce que no necesita encontrarse escrito un documento jurídico para ser reconocido como tal, así dentro de los documentos jurídicos encontramos principalmente dos clases, los de representación material y los de representación literal. Son documentos literales, aquéllos en los que la representación se realiza a través de la escritura, y documentos materiales todos aquéllos que no puedan ser considerados como literales, como por ejemplo las fotografías.³⁰

Siguiendo este orden de ideas, el Código de Procedimientos Civiles para el Distrito Federal (CPCDF) en su artículo 289 antes de las reformas publicadas el 10 de enero de 1989 enumeraba los medios de prueba, a saber:

1. La confesión.
2. Los documentos públicos y privados.
3. Los dictámenes periciales.
4. El reconocimiento o inspección judicial.
5. El testimonio de terceros.
6. Las fotografías, copias fotostáticas, registros dactiloscópicos y, en general, todos aquellos elementos aportados por los descubrimientos de la ciencia.
7. La fama pública.
8. Las presunciones.
9. Los demás medios que produzcan convicción en el juzgador.

²⁹ Davara Rodríguez citado por García Aguilar, Nicolás. “La cuestión de la responsabilidad en el Derecho Informático”. REDI: Revista Electrónica de Derecho Informático. Disponible [Online]: <<http://derecho.org/redi/>>

³⁰ Alsina citado por Ovalle Favela, José. “Derecho Procesal Civil”. Harla, séptima edición, México, 1995, pág. 133.

De conformidad con la enumeración anterior dentro del CPCDF se consideraba que los documentos públicos y privados eran diferentes a las fotografías, copias fotostáticas, registros dactiloscópicos y, a todos los elementos atribuibles a la evolución de la ciencia. Así, éstos últimos fueron considerados como “documentos técnicos” (prueba documental técnica) correspondiendo a los documentos materiales. Requiriendo, en general, esta prueba que quien la presente suministre al tribunal de los aparatos o elementos necesarios para que pueda apreciarse el valor de los registros y reproducirse los sonidos y figuras (artículos 373 a 375). Tomando en consideración lo puntualizado hasta el momento no existe ninguna dificultad para afirmar que algunos documentos electrónicos pueden ser documentos materiales (como aquéllos que reproducen sonidos), pero los documentos digitales “escritos” deben ser considerados como documentos literales.

Los documentos públicos y privados se encuadraron dentro de la “prueba instrumental” (prueba documental literal), la cual contiene a los documentos escritos, a los literales. Los documentos escritos a su vez se subdividen en públicos y privados. En cuanto a considerar a los documentos literales como documentos electrónicos será necesario hacer un estudio que comprenda a los documentos públicos y a los privados por separado.

A) Documentos públicos.

Las subdivisión de los documentos literales en públicos y privados se da en relación a los sujetos (autores) del documento, ya que el autor tiene esencial importancia en cuanto a la fidelidad del documento. Siendo el momento crítico para el establecimiento de la fidelidad del documento su acto de formación; uno de los medios para garantizar esa fidelidad es que en ese acto participe una persona que ofrezca garantías morales e intelectuales que permitan evitar la mayor parte de los errores de inteligencia y de voluntad en la formación misma, surgiendo así los documentos públicos contrapuestos a los privados.³¹

Los documentos públicos son los otorgados por autoridades o funcionarios públicos en el ejercicio de sus atribuciones o por profesionales investidos de fe pública, dentro del ámbito de su competencia y en forma legal.

Siendo la fe pública una facultad, una atribución que se confiere a determinados funcionarios, a los que se les otorga una confianza oficial para que certifiquen y para que atestigüen con un testimonio de calidad y, sobre todo, con un atestiguamiento sancionador. Estas personas que están investidas de fe pública pueden ser algunos funcionarios públicos, los Notarios Públicos, los corredores públicos y los secretarios judiciales, entre los cuales, desde luego, están los actuarios.³²

De donde emana que los documentos públicos tengan una presunción de autenticidad (aunque ésta puede ser desvirtuada por medios legales), y que por regla general, hagan prueba plena (artículo 403 CPCDF).

³¹ Canelutti, Francesco. Ob. cit., p.p. 100 y 101.

³² Gómez Lara, Cipriano. Ob. cit., pág. 145.

Así, resulta perfectamente posible que un documento electrónico pueda ser considerado como un documento público siempre que llene las características antes señaladas.

El CPCDF enuncia en su artículo 327 a los documentos públicos a saber:

I. Las escrituras públicas, pólizas y actas otorgadas ante Notario o corredor público y los testimonios y copias certificadas de dichos documentos;

II. Los documentos auténticos expedidos por funcionarios que desempeñen cargo público en lo que se refiera al ejercicio de sus funciones;

III. Los documentos auténticos, libros de actas, estatutos, registros y catastros que se hallen en los archivos públicos, o los dependientes del gobierno federal, de los Estados, de los Ayuntamientos o del Distrito Federal;

IV. Las certificaciones de las actas del estado civil expedidas por los jueces del Registro Civil, respecto a constancias existentes en los libros correspondientes;

V. Las certificaciones de constancias existentes en los archivos públicos expedidas por funcionarios a quienes compete;

VI. Las certificaciones de constancias existentes en los archivos parroquiales y que se refieran a actos pasados antes del establecimiento del Registro Civil, siempre que fueren cotejadas por Notario Público o quien haga sus veces con arreglo a derecho;

VII. Las ordenanzas, estatutos, reglamentos y actas de sociedades o asociados, universidades, siempre que estuvieren aprobados por el gobierno Federal o de los Estados, y las copias certificadas que ellos expidieren;

VIII. Las actuaciones judiciales de toda especie;

IX. Las certificaciones que expidieren las bolsas mercantiles o mineras autorizadas por la ley y las expedidas por corredores titulados con arreglo al Código de Comercio;

X. Los demás a los que se les reconozca ese carácter por la ley.

B) Documentos privados.

Los documentos privados en oposición a los públicos se definen como aquéllos que no tienen el carácter de públicos, como aquéllos que provienen de particulares sin la intervención de funcionarios o autoridades públicas o de persona autorizada para ejercer la fe pública.

El artículo 334 del CPCDF enuncia a los documentos privados de forma incompleta al indicar que "Son documentos privados los vales, pagarés, libros de cuentas, cartas y demás escritos firmados o formados por las partes o de su orden y que no estén autorizados por escribanos o funcionario competente".

En cuanto a considerar al documento electrónico en sentido estricto como documento privado la doctrina aún tiene algunas reservas fundamentadas en que falta el requisito de la firma necesario en todo documento privado. Es decir, el imponer el nombre propio y el apellido por parte de la persona de donde emana determinada manifestación de voluntad y que implica su conformidad con lo escrito. Tratándose de los documentos electrónicos en sentido amplio esta reserva no se aplica, debido a que una vez impresos pueden ser

firmados por las partes (en este caso la única oposición se haría en el supuesto de que se requiriera que sean de formación autógrafa).

Sin embargo, en cuanto a la firma primeramente aparece una divergencia doctrinal en cuanto a su necesidad. Algunos autores consideran que no es necesario que los documentos privados se encuentren firmados cuando el Derecho positivo no lo exija. Siguiendo esta corriente doctrinal no existiría objeción alguna para reconocer al documento electrónico en sentido estricto como documento privado, sin embargo, la mayoría de la doctrina manifiesta que el documento privado debe ser firmado por los otorgantes al ser la firma el signo que demuestra que se acepta lo escrito y se reconoce como propio; sin la firma el documento es un documento anónimo, careciendo de autenticidad.

En nuestra opinión y siguiendo el pensamiento de Carnelutti³³ consideramos que la suscripción es un elemento básico del documento privado, por lo que el escrito anónimo, no suscrito, no es un verdadero documento.

Surgiendo una importante dificultad con el documento electrónico, ya que éste es incompatible con la firma manuscrita, ante lo cual se ha dado como solución la homologación de la firma tradicional con la firma digital, la cual tiene la misma función que la primera en cuanto a la suscripción; ambas señalan al autor del documento (función indicativa), si éste asume la paternidad del documento (función declarativa) y permiten verificar si el que firma es el que se indicó en la suscripción (función probatoria). Sin embargo, las firmas electrónicas, por su desconocimiento aún no son del todo aceptadas, incluso se ha llegado a decir que una firma de puño y letra (autógrafa) da mayor seguridad que una firma electrónica, ya que cada individuo firma de modo diferente siendo su firma de difícil reproducción.

De donde se deriva que el documento electrónico no podrá ser considerado como documento privado sino hasta que se homologue la firma manuscrita a la electrónica, lo cual se dará en un futuro no muy distante, al no existir razón alguna que lo impida como se demostrará en el punto 3.7. de esta tesis.

En nuestro país ya existen algunos ordenamientos legales que hacen referencia expresa al documento electrónico y a los medios electrónicos y telemáticos como son:

El Código de Comercio en su artículo 48 aunque hace alusión a los documentos electrónicos como copias de cartas y otros documentos que los comerciantes expidan, o reciban (que no estén incluidos en el artículo 49). Establece algunos de los elementos a los que ya hemos hecho referencia como son que permitan su reproducción posterior íntegra y su consulta o compulsas en caso necesario.

El Código Financiero del Distrito Federal en su artículo 84 fracción VII inciso a) hace referencia a los libros o registros que forman parte de la contabilidad solicitados en el curso de la visita, cuando se lleve ésta de forma electrónica, debiéndose presentar ésta de

³³ Carnelutti, Francesco. Ob. cit., pág. 90.

inmediato, así como los diagramas y el diseño del sistema de registro electrónico, en su caso.

Por su parte, el artículo 459 establece las reglas a seguir en el caso de las entidades que utilicen sistemas de registro electrónico de contabilidad, a saber: Obtener de la Secretaría la autorización por escrito para la utilización en sus libros principales de contabilidad; comunicar por escrito, las características y especificaciones del sistema, señalando entre otros, marca del equipo, capacidad y características de las máquinas, lenguajes que utilicen, descripción de los programas a emplear y balanza de comprobación de saldos a la fecha en que se adopte este tipo de registro; y los cambios de sistema, entre otros. Indicándose en el artículo 489 que las entidades que lleven a cabo el registro de sus operaciones financieras y presupuestales en sistemas de procesamiento electrónico de datos, deberán suministrar la información requerida por la Secretaría para la elaboración de la Cuenta Pública, en la forma y medios por ella señalados.

En la Ley de Comercio Exterior en el artículo 84 se prescribe que las notificaciones se harán a la parte interesada o a su representante a través de cualquier medio directo como el de mensajería especializada o electrónico.

En la Ley del Impuesto sobre la Renta una vez más se hace mención expresa en los artículos 58 fracción X, 112 fracción VIII, 72 fracción III, y 119-I fracción VII a la contabilidad mediante el sistema de registro electrónico, en cuyo caso la información requerida deberá proporcionarse en dispositivos magnéticos procesados en los términos que señale la Secretaría de Hacienda y Crédito Público, mediante disposiciones de carácter general.

La Ley Aduanera en su artículo 38 prescribe el empleo de un sistema electrónico con grabación simultánea en soportes magnéticos para el despacho de las mercancías en los términos que la Secretaría establezca, e incluso menciona el uso de una clave electrónica confidencial correspondiente al agente o apoderado aduanal en las operaciones grabadas en los medios magnéticos en los que aparezca la clave electrónica confidencial y a un código de validación generado por la aduana; casos en los que se considera sin que se admita prueba en contrario que fueron efectuados por el agente o apoderado aduanal al que corresponda dicha clave; la clave electrónica confidencial de los agentes y apoderados aduanales equivale a la firma autógrafa.

En el artículo 45 del Código Fiscal de la Federación al tratar de la visita domiciliaria también se hace referencia a la contabilidad llevada mediante el sistema de registro electrónico o que se grabe en discos ópticos o en cualquier otro medio que autorice la Secretaría de Hacienda y Crédito Público, mediante reglas de carácter general. Y se agrega que en estos supuestos los visitados deberán poner a disposición de los visitantes el equipo de cómputo y sus operadores, para que los auxilien en el desarrollo de la visita.

En los artículos 27 y 123 de la Ley Federal del Derecho de Autor se hace referencia no sólo al documento electrónico como soporte de una obra sino también a los medios de telecomunicaciones como forma de difusión de la misma.

Por su parte, la antigua Ley del Seguro Social en el artículo 19 último párrafo regulaba la posibilidad de que el patrón lleve la contabilidad mediante el sistema de registro electrónico, permitiéndole que proporcione información como altas y bajas de los trabajadores, las modificaciones de sus salarios (y las que señale esta ley y sus

Reglamentos), entre otros, en dispositivos magnéticos procesados en los términos que señale el Instituto.

3.5. El documento heterógrafo.

El hecho representado en un documento puede o no ser un hecho humano, tratándose de documentos heterógrafos o autógrafos se trata necesariamente de un hecho humano, ya que esta clasificación se da en cuanto si al autor del documento es o no la misma persona que realizó el hecho humano. En cuanto a la persona que forma el documento no se toma en cuenta propiamente a quien lo realiza materialmente sino respecto del cual se verifican los efectos legales de la formación misma. Siendo los documentos heterógrafos aquéllos cuya nota esencial consiste en que no están formados por quien realiza el hecho documentado.³⁴

3.6. El documento autógrafo.

Por su parte, el documento autógrafo surge cuando "quien manifiesta el pensamiento realiza los actos que el orden jurídico considera suficientes para atribuirle los efectos de la formación de la escritura"³⁵, es decir, el documento autógrafo representa un hecho de la persona misma que lo forma, obviamente esto solo puede acontecer cuando el documento represente el hecho de su formación. La formación del documento es un hecho que se individualiza dentro de la persona, tiempo y lugar. Reduciéndose el problema de la formación a: por quién fue formado, dónde y cuándo. Si el documento no es medio para responder alguna de éstas preguntas no suministra prueba respecto de ese aspecto de su formación, al ser un documento incompleto.³⁶

a) Autenticidad.

Otro elemento del documento autógrafo es la autenticidad. Desde tiempo lejano el hombre ha tratado de garantizar la autenticidad, para lo cual ha recurrido a diversos mecanismos y/o procedimientos, por ejemplo, las firmas, los papeles especiales, etcétera.

En la doctrina mexicana la autenticidad implica que en el documento debe corresponder el autor aparente con el autor real del mismo, "La autenticidad es, en realidad, una indubitabilidad, es decir, el no poder dudar del origen y de la procedencia de un documento".³⁷ Sin embargo, en numerosas ocasiones la doctrina internacional también integra dentro de la autenticidad que el documento no debe haber sufrido alteraciones desde su suscripción (integridad), y que debe haber sido otorgado por el autor de la manera exacta en la que se manifestó su voluntad (no repudio).

³⁴ *Ibidem*, pág. 88.

³⁵ *Ibidem*, pág. 89.

³⁶ *Ibidem*, pág. 95.

³⁷ Gómez Lara, Cipriano. *Ob. cit.*, pág. 145.

b) La suscripción.

La suscripción en el documento autógrafo resulta esencial, ya que "Un acto humano no puede ser representado más que cuando se indique su autor, precisamente porque se trata de una entidad concreta que, en substancia, se reduce al hombre que obra".³⁸

La suscripción indica al autor del documento convirtiéndose en un elemento del documento autógrafo. De donde se deriva que no todo escrito es un documento, ya que a la forma escrita le falta la forma representativa, para lo cual es necesario que se reconozca al autor del mismo, lo cual se hará de conformidad con las formas eficaces para esa indicación establecidas en el Derecho positivo mexicano.

El documento electrónico al ser incompatible con la firma autógrafa destruyó la noción de suscripción tradicionalmente aceptada pero introdujo nuevos métodos para controlar la autenticidad del documento que incluso pueden considerarse superiores al criterio tradicional de la suscripción, al ofrecer más garantías que los reconocimientos efectuados directamente por el hombre.

c) La data.

La data del documento autógrafo consiste, en la indicación del lugar y del tiempo de su formación. Si el documento no hace fe de su autor debe al menos hacerlo de su data o no servirá para probar aspecto alguno de su formación.³⁹

3.7. La firma electrónica.

La noción de firma electrónica adquiere relevancia en la actualidad al darse el equiparamiento del documento digital con el privado, y en especial en cuanto a los contratos entre ausentes, lo que ha acarreado como consecuencia que se haya tenido que extender el concepto de firma manuscrita a cualquier método que permita la eficiente identificación del emisor de una manifestación de voluntad. Sin embargo, algo que resulta relativamente sencillo en el mundo real como es el firmar, adquiere complicados relieves técnicos en cuanto al mundo virtual, donde para obtener una firma digital se requiere el uso de la criptografía y de algoritmos matemáticos.

A pesar de que en la mayoría de las legislaciones aún no se ha realizado la homologación entre firma digital y firma autógrafa, la mayoría de los países ya reconocen la necesidad de regular la aceptación de la firma digital lo más pronto posible, ya que ella permitirá el correcto desarrollo del comercio electrónico y de todo acto jurídico susceptible de realizarse por medios virtuales, como los contratos. Por ello, se han creado entidades certificadoras públicas y privadas, para expedir certificados de clave pública a numerosos usuarios que usan sus claves en las comunicaciones telemáticas.

³⁸ Carnelutti, Francesco. Ob. cit., pág. 90.

³⁹ Ibidem, p.p. 94 y 95.

El número de éstas entidades ha crecido rápidamente alrededor del mundo, pero aún existe incertidumbre en cuanto a si podrán ofrecer la seguridad necesaria a las transacciones electrónicas debido a que se basan en tecnología de creación reciente.

En cuanto a las firmas digitales en sí, se han considerado diversas técnicas para su implementación siendo las criptográficas las que han tenido mejor resultado y mayor garantía de seguridad. Pero siempre se aconseja su uso conjunto con otras medidas de seguridad como los códigos secretos, la biometría, y/o algunas otras de las señaladas en el punto 3.3. de la presente investigación. Desgraciadamente, ninguna de ellas puede considerarse como de fácil acceso para la generalidad de la población (principalmente debido a su costo y a las características de su implementación).

Las firmas electrónicas basadas en criptografía,⁴⁰ se iniciaron como criptografía simétrica (uso de una sola clave para encriptar y desencriptar) pero para brindar aún más seguridad se implementó la criptografía asimétrica; existiendo dos claves complementarias, una conocida públicamente (pública) y otra secreta (privada) conocida únicamente por el suscriptor quien es responsable de su guarda, cada una de las cuales desbloquea o desencripta el código generado por la otra, mediante procedimientos automáticos efectuados por un software especial.

En caso de la realización de un acto jurídico con uso de la firma electrónica, el emisor deberá utilizar la llave pública del destinatario para encriptar un mensaje dirigido a esa persona, y firmarlo electrónicamente con su propia clave privada. El destinatario utilizará su llave privada para desencriptarlo, y se comunicará con el registro o repositorio donde se encuentre el certificado correspondiente para conocer la clave pública del emisor; lo que permitirá que el destinatario verifique la firma (clave privada) de éste con la llave pública del mismo. Posteriormente el destinatario firmará digitalmente el documento electrónico con su clave privada y lo enviará al emisor.

Así, una operación común con firma digital comienza con la determinación por parte del firmante del contenido del documento que corresponde a su manifestación de voluntad (mensaje plano), luego el software crea un resumen del mensaje mediante la aplicación de la función "hash function" obteniéndose como resultado un código único para el mensaje denominado "hash result"; si el mensaje cambia el "hash result" será diferente. Por último, el software encripta el "hash result" con la clave privada del firmante. La firma electrónica así obtenida es única tanto para el mensaje como para la clave privada utilizada en su creación.

La verificación de la firma digital es realizada computando un nuevo "has result" del mensaje original utilizando la misma "hash function" usada en la creación de la firma digital. Finalmente, con la clave pública que surge del certificado de clave pública del firmante, el receptor comprueba si la firma digital efectivamente proviene de la clave privada del firmante y si el nuevo "hash result" es igual al que proviene de la firma digital, en cuyo caso se tiene un documento digital integro y auténtico.

⁴⁰ Rama de las matemáticas que se ocupa de transformar mensajes en formas aparentemente inteligibles y devolverlas a su forma original.

Una vez tratado lo anterior se puede definir a la firma digital como un valor numérico que se adhiere a un mensaje de datos transformándolo y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.⁴¹

En la anterior definición y de conformidad con el Proyecto de Ley No. 227 de abril de 1998 de Colombia, se decide que la tecnología a utilizar será la criptográfica.⁴² Éste Proyecto de Ley señala que debe entenderse por mensaje de datos toda información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, el intercambio electrónico de datos (EDI)⁴³ o el correo electrónico.

Al respecto, la Comisión de las Naciones Unidas Sobre Derecho Mercantil Internacional (CNUDMI) ha propuesto el establecimiento de una red única de claves o huellas públicas certificadas ante fedatarios públicos autorizados para tal efecto, permitiendo el uso de las firmas digitales como elementos suficientes para demostrar que determinadas personas celebraron por su propia voluntad y libres de todo vicio del consentimiento uno o varios actos jurídicos.⁴⁴

En México es el Comité Mexicano de Seguridad EDI, presidido por el Banco de México, el que utilizando las propuestas de la CNUDMI, desarrolla en este momento un sistema criptográfico asimétrico y su infraestructura para obtener, registrar y certificar ante Notario Público firmas digitales únicas, que servirán en primera instancia para identificar plenamente a los usuarios del sistema Edi-México Comercial. Para lograr este objetivo se deberá realizar la adaptación de los ordenamientos jurídicos contractuales a las exigencias del mundo virtual y de la aldea global, y obtener la aceptación de fórmulas modernas como las firmas digitales y los documentos electrónicos como medio probatorio de plena validez jurídica.

Mientras que la Directiva del Parlamento Europeo y del Consejo de la Unión Económica Europea sobre Firma Electrónica (mayo de 1998)⁴⁵, reconoce que la firma electrónica es esencial para fomentar la seguridad y confianza en las redes abiertas, incluyendo en su propuesta que en cuanto a firma digital se debe establecer una política común para todos los países europeos, terminando con lo que se venía dando hasta el momento que era que cada país (por ejemplo: Alemania, Italia, Reino Unido) desarrollará su propia legislación al respecto.

⁴¹ Proyecto de Ley No. 227 de abril 21 de 1998, por medio del cual se define y reglamenta el acceso y uso del comercio electrónico, firmas digitales y se autorizan las entidades de certificación. Colombia. Disponible [Online]: <http://www.qmw.ac.uk/tl6345/colombia_sp.htm

⁴² Idem.

⁴³ El Intercambio Electrónico de Datos implica la transmisión electrónica de información de una computadora a otra estando estructurada la información conforme a alguna norma técnica convenida al efecto.

⁴⁴ Kemper, Ana María. Ob. cit.

⁴⁵ Idem.

En Colombia, como ya se mencionó, el uso de la firma digital se regula mediante el Proyecto de Ley No. 227 de abril de 1998⁴⁶, en el que se define y reglamenta el uso del comercio electrónico, firmas digitales y se autorizan las entidades de certificación. De igual forma, en la Ley del Estado de Utah sobre la Firma Digital (Utah Digital Signature Act), que comenzó a regir el 1 de mayo de 1995 y en la Guía de Firma Digital (Digital Signature Guidelines), publicada en octubre de 1995 por The American Bar Association's Information Security Committee (Asociación de la Barra Americana del Comité de Seguridad de la Información), se establece el sistema regulatorio aplicable a la firma digital.⁴⁷ En el caso de Estados Unidos la Ley del Estado de Utah fue y es la ley modelo para la creación de otras leyes de la misma naturaleza en los demás Estados de ese país. Por su parte, en el Proyecto de Ley de Firma Digital Alemana (SigG)⁴⁸ se equipará la firma ológrafa a la digital y se crean las condiciones generales para que las firmas digitales puedan considerarse seguras, permitiendo que las falsificaciones de firmas digitales y de información firmada puedan ser verificadas sin lugar a dudas. Sin embargo, se permite a criterio de los interesados el uso de otras medidas de seguridad.

En los países a los que antes se hizo mención y que han regulado al respecto, en cuanto a las firmas digitales se han establecido parámetros similares, a saber:

La "Revolución Digital" ha traído consigo la tendencia a la automatización y eliminación de papel, implementando modernas tecnologías como la del documento electrónico y la firma digital, la cual es "susceptible de la misma o superior garantía de confianza que la firma ológrafa".⁴⁹

Siempre que se prevea la utilización de la firma digital es necesario crear una infraestructura de firma digital con el propósito de establecer las condiciones de un uso confiable del documento firmado por medios electrónicos. Dicha infraestructura será compuesta por un Organismo Licenciante, un Organismo Auditante, Autoridades Certificantes Licenciadas, el Suscriptor, el sello de fecha y hora, la Firma Digital, los componentes técnicos, y el Certificado de Clave Pública. A continuación se dará una breve descripción de cada uno de ellos:

Organismo Licenciante.

El Organismo Licenciante es un órgano administrativo que tendrá como principales funciones:

El otorgar, denegar y revocar licencias habilitantes para acreditar a las Autoridades Certificantes Licenciadas y emitir los correspondientes certificados de clave pública, que permitirán verificar las firmas digitales de los certificados que éstas emitan;

⁴⁶ Proyecto de Ley No. 227. Ob. cit..

⁴⁷ Ramos Suárez, Fernando. "La firma digital". REDI: Revista Electrónica de Derecho Informático, número 9, abril, 1999. Disponible [Online]: <<http://derecho.org/redi/>>

⁴⁸ "Borrador del Proyecto de Ley de Firma Digital Alemana (SigG)". Traducción por Kurner, Christopher. Disponible [Online]: <<http://www.firma.gov.ar/firma.html>>

⁴⁹ Decreto No. 427 del Ejecutivo del 16 de abril de 1998. Argentina. Ob. cit..

Verificará que las Autoridades Certificantes Licenciadas utilicen sistemas técnicamente confiables, que dichas Autoridades sean confiables (que puedan garantizar que cumplirán con los requerimientos legales relevantes para operar como Autoridad Certificadora Licenciada), posean el conocimiento necesario (que las personas que trabajen para ellas tengan el conocimiento, la experiencia y la calificación necesarias), y estén registradas en un plan de seguridad, aprobado por el Organismo Licenciante;

Aprobará el manual de procedimientos, los reglamentos internos de la prestación del servicio (así como sus reformas), el plan de seguridad y el cese de actividades presentados por las Autoridades Certificantes;

Impondrá sanciones; y

Podrá incluir en la licencia cuantas cláusulas complementarias considere necesarias para asegurar que la Autoridad Certificadora Licenciada cumpla con sus obligaciones.

Dentro de sus obligaciones se encuentran el evitar tener conocimiento de la clave privada de cualquier suscriptor de los certificados que emita; mantener control sobre su propia clave privada; y permitir el acceso público permanente a los certificados de clave pública y a la lista de certificados revocados por medio de conexiones de telecomunicaciones (de preferencia por sistemas On-line) públicamente accesibles; por el mismo medio debe hacer del conocimiento público las direcciones, nombres y números telefónicos de las Autoridades Certificantes Licenciadas.

Organismo Auditante.

El Organismo Auditante, es un órgano administrativo cuya función esencial será la de auditar periódicamente al Organismo Licenciante y a las Autoridades Certificantes Licenciadas; encontrándose dentro de sus obligaciones el utilizar técnicas de auditoría apropiadas en sus evaluaciones; evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como el cumplimiento con las especificaciones del manual de procedimientos y el plan de seguridad aprobados por el Organismo Licenciante; verificar que se utilicen sistemas técnicamente confiables; y emitir informes de auditoría con los hallazgos, conclusiones y recomendaciones en cada caso.

En algunas legislaciones el órgano administrativo que funge como Organismo Licenciante también posee las obligaciones del Organismo Auditante.

Autoridades Certificantes Licenciadas, o Autoridades Certificadoras, o Terceras Partes Confiables.

En el Proyecto de Ley sobre Documentos Electrónicos de la República de Chile⁵⁰ se establece en principio que son los Notarios Públicos los únicos autorizados para actuar

⁵⁰ Proyecto de Ley sobre Documentos Electrónicos de la República de Chile. CENIT: Centro de Investigaciones en Information Technology-Estudio Jara, Del Favero y Cia.. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

como Autoridad Certificadora, pero después se indica que puede darse cumplimiento a las normas correspondientes a las funciones de la Autoridad Certificadora a través de intermediarios.

En el resto de las legislaciones se atribuye el rango de Autoridad Certificante Licenciada a una persona física o moral, pública o privada facultada para emitir o revocar certificados de clave pública, y que sólo podrá operar mediante licencia otorgada por el Organismo Licenciante.

Sin embargo, en México, el proyecto de infraestructura de firma digital en desarrollo por el Comité Mexicano de Seguridad prevé que la obtención, registro y certificación de firmas electrónicas serán realizados por Notario Público.

La Autoridad Certificante Licenciada deberá: poseer y acreditar el acceso a hardware y software suficientemente confiable; tener personal con los conocimientos y experiencia necesaria; contar con los elementos técnicos necesarios para la generación de firmas digitales; tener los elementos propios para la emisión de certificados, su conservación y publicidad, así como para la conservación y archivo de documentos digitales; y obtener la autorización (licencia) correspondiente.

Dentro de sus principales obligaciones se encuentran: el poseer un certificado del Organismo Licenciante; publicar su clave pública; evitar tener conocimiento de la clave privada del suscriptor y mantener el control de su propia clave privada; operar utilizando un sistema técnicamente confiable e implementar sistemas de seguridad efectivos para garantizar la emisión y creación de firmas digitales, y la conservación y guarda del archivo de certificados y documentos digitales; deberá mantener la publicidad de los registros de claves pública en medios telemáticos, de preferencia en línea (On-line); tendrá que poseer un registro (repositorio) que contenga los certificados emitidos así como los revocados; deberá mantener una actualización permanente de sus medios técnicos; garantizar la protección y debido uso de la información proporcionada por el suscriptor; garantizar la prestación del servicio de forma permanente; suministrar la información que le requieran las entidades administrativas o judiciales competentes; ofrecer los servicios de archivo y conservación de documentos electrónicos; poner a disposición del suscriptor el correspondiente certificado de clave pública, así como toda la información relativa a la tramitación del certificado; verificar y establecer fehacientemente la identidad de la persona y de los representantes legales que corresponda en su caso; deberá permitir visitas de inspección de los organismos encargados para realizarlas; informar al solicitante las medidas necesarias para asegurar su firma digital y su verificación confiable, debiendo señalar que la información con firma digital puede necesitar ser refirmada, y que el valor de seguridad de una firma digital decrece con el tiempo (en este aspecto todavía no se ha podido señalar con certeza en cuanto tiempo y mediante que procedimientos se deberá otorgar una nueva firma digital); debe informar inmediatamente al Organismo Licenciante en caso de cese de actividades o de un procedimiento de declaración de quiebra o de suspensión de pagos; y cumplir cualquier otro requisito determinado por éste Organismo.

En el Proyecto de Ley de Firma Digital Alemana⁵¹ en cuanto a la publicación de certificados se permite obviar esta obligación si existe un pedido explícito de no

⁵¹ "Borrador del Proyecto de Ley de Firma Digital Alemana (SigG)". Ob. cit..

publicación por parte del suscriptor. Asimismo, se permite al suscriptor registrar un seudónimo en vez de su nombre, en especial en el caso de aquellos nombres que pueden ser confundidos con otros.

La licencia de la Autoridad Certificante se revoca en caso de no cumplir con sus obligaciones o con los requisitos estipulados, en cuyo caso el Organismo Licenciente transfiere los certificados a otra Autoridad Certificante o los revoca, principalmente en caso de que se sospeche que los mismos han sido alterados o su seguridad se ha visto comprometida de alguna forma.

Para que la Autoridad Certificante Licenciada pueda emitir certificados de clave pública es necesario que reciba del futuro suscriptor una solicitud de emisión de certificado de clave pública, la cual deberá estar firmada digitalmente con la correspondiente clave privada; en la mayoría de las legislaciones son las Autoridades Certificantes Licenciadas las que generan las llaves pública y privada del suscriptor y se las entregan en un medio físico (tarjeta inteligente u análogo), pero en la Ley del Estado de Utah sobre la Firma Digital se prevé que una vez generadas éstas claves se lleven a la Autoridad Certificante para que otorgue el correspondiente certificado.

Suscriptor de certificado de clave pública o firmante.

El suscriptor es la persona a cuyo nombre se emite un certificado y que es titular de la clave privada correspondiente a la clave pública incluida en dicho certificado. Él mantendrá bajo su estricto y exclusivo control el procedimiento para generar su firma digital, y tiene como principales obligaciones el recibir las claves por parte de la Autoridad Certificante Licenciada, o generar las claves utilizando el sistema de seguridad exigido por ésta Autoridad; proveer todos los datos requeridos por la Autoridad Certificante Licenciada bajo declaración jurada; mantener el control de su clave privada; e informar inmediatamente a la Autoridad Certificante Licenciada sobre cualquier circunstancia que pudiere haber comprometido su clave privada, solicitando la revocación del certificado correspondiente.

Los suscriptores son responsables por la falsedad o error en la información suministrada a la Autoridad Certificante Licenciada, y en los casos en que no den oportuno aviso de revocación de los certificados.

Se entenderá que el suscriptor acepta el certificado desde el momento en que éste o una persona en su nombre lo ha publicado o lo ha enviado a una o más personas. Desde el momento de la aceptación, el suscriptor garantiza a todas las personas de buena fe que se soportan en la información contenida que: la firma digital autenticada mediante el certificado está bajo su control exclusivo; que ninguna persona ha tenido acceso al procedimiento de generación de la firma digital; y que la información contenida en el certificado es verdadera y corresponde a la suministrada por él a la Autoridad Certificante Licenciada.

Certificado de clave pública o certificado.

El certificado de clave pública es una certificación rotulada con una firma digital respecto a la atribución de una clave de firma pública a una persona; es el documento digital (registro electrónico) emitido y firmado digitalmente por una Autoridad Certificante Licenciada (o en su caso por el Organismo Licenciante), que asocia una clave pública con su suscriptor durante el periodo de vigencia del certificado. Su principal función es la de vincular el par de claves con el firmante de tal forma que quien pretenda verificar una firma digital con la clave pública que surge de un certificado, tenga la seguridad que la correspondiente clave privada es detenada por el firmante. Así, para que un par de llaves pueda ser utilizada válidamente, deberá contar en forma adjunta con un certificado electrónico de llave pública.

Un certificado de clave pública como mínimo debe contener el nombre (marcado con una anotación adicional si existe posibilidad de confusión o con el uso de un seudónimo inequívoco atribuible al dueño de la clave), y domicilio del suscriptor; identificación del suscriptor nombrado en el certificado; tipo de certificado; número de licencia, en el caso de certificados emitidos para Autoridades Certificantes Licenciadas; el nombre, y la dirección donde realiza sus actividades la Autoridad Certificante Licenciada que emite el certificado (o en su caso del Organismo Licenciante); clave pública utilizada por el suscriptor; la metodología para verificar la firma digital del suscriptor; información acerca de la limitación de uso de la clave de firma a determinados tipos y ámbitos de aplicación; número de serie del certificado; periodo de vigencia del certificado; y firma digital de la Autoridad Certificante Licenciada (o del Organismo Licenciante en su caso) que emite el certificado.

El certificado sólo será válido si ha sido emitido por una Autoridad Certificante Licenciada (o por el Organismo Licenciante), no ha sido revocado, y no ha expirado.

En los certificados la recopilación de información de un tercero está permitida siempre que la persona afectada de su consentimiento y sólo podrá usarse para los fines que considere propios el afectado.

En el caso de que el suscriptor utilice un seudónimo, la Autoridad Certificante Licenciada deberá transmitir la información concerniente a su identidad ante el pedido de autoridades competentes.

Los certificados se inscriben en un registro, o repositorio (*repository*) que consiste en una base de datos a la que el público puede acceder por medios telemáticos, de preferencia en línea para conocer acerca de la validez de los mismos. Y se recomienda que las claves privadas de los usuarios sean encriptadas vía software o conservadas en un medio físico como smart cards o PC cards.

En la Ley de Utah se establece que la Autoridad Certificante puede emitir diferentes tipos de certificados (debiendo el interesado solicitar aquél adecuado a sus intereses):

- ◆ Los de identificación. Identifican un nombre y lo conectan con una clave pública.

- ◆ Los de autorización. Proveen información del firmante como dirección comercial, antecedentes, catálogos de productos, etcétera. Esto por ejemplo, podría ser solicitado para una operación financiera en la que se necesitara saber los estados financieros y antecedentes criminales del firmante, en cuyo caso no sería suficiente usar un certificado de identificación.
- ◆ Los notariales. La Autoridad de Certificación actúa como un Notario Público.
- ◆ Los Digital Time-Stamp Certificates. Permiten determinar el día y la hora en que el documento fue digitalmente firmado.

Los certificados de clave pública se pueden revocar a solicitud del suscriptor, o de un tercero (si contiene información de éste o es persona o autoridad legalmente facultada para ello); o si el certificado se basa en información falsa, si deja de ser técnicamente confiable, o si la Autoridad Certificante Licenciada cesa en sus actividades o se revoca su licencia y no transfiere los certificados a otra Autoridad Certificante Licenciada o al Organismo Licenciante, por muerte del suscriptor, por disolución del suscriptor en el caso de personas jurídicas, por incapacidad sobrevenida del suscriptor, por quiebra del suscriptor, o si la clave privada de la Autoridad Certificante Licenciada o su sistema de seguridad han sido comprometidos de manera que afecte la confiabilidad del certificado. La revocación deberá establecer el momento desde el cual se aplica y no podrá ser retroactiva.

Los certificados de firmas digitales emitidos por Autoridades Certificantes Licenciadas u Organismos Licenciantes extranjeros debidamente autorizados, y que garanticen los certificados por ellos expedidos en forma equivalente a los establecido en esta infraestructura de firma digital, en cuanto a su contenido, validez y vigencia, podrán ser reconocidos en los mismos términos y condiciones exigidos en ésta infraestructura digital para la emisión de certificados por parte de las Autoridades Certificantes Licenciadas nacionales.

En el Proyecto de Firma Digital Alemana para que este reconocimiento de certificados extranjeros se dé, se necesita de la suscripción de acuerdos internacionales relativos al reconocimiento de certificados.

Sello de fecha y hora.

El sello de fecha y hora, se da debido a que la Autoridad Certificante Licenciada debe rotular la información digital con un sello digital de fecha y hora que indica en que tiempo fue presentada dicha información.

Firma digital.

En el caso de la firma digital, para que ésta pueda tener la misma fuerza y efectos que la firma manuscrita deberá ser una sola persona la que la use; ser susceptible de ser verificada; estar bajo control exclusivo del suscriptor; estar ligada a la información o mensaje contenido en el documento electrónico de tal manera que si éstos son cambiados, la firma digital es invalidada; y cumplir con toda estipulación legal que le sea aplicable.

La firma digital es resultado de una transformación de un documento digital empleando un criptosistema asimétrico y un digesto seguro, de tal forma que una persona que posea el documento digital inicial y la clave pública del firmante puede con certeza saber:

* Si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante, lo cual impide su repudio y garantiza su autenticidad.

* Si el documento digital ha sido modificado desde el momento de su firma, lo que garantiza su integridad, siendo la integridad la condición de no alteración de un documento digital; salvo en el caso de la adición de un endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El documento será tanto más seguro cuanto más difícil sea alterarlo.

La utilización de un criptosistema asimétrico como se explicó en el punto 3.3.1. implica que se emplea un algoritmo que utiliza un par de claves, una clave privada y su correspondiente clave pública. Debiendo ser ese criptosistema asimétrico técnicamente confiable.

La clave privada es el “conjunto de datos únicos e inalterables generados en base a un procedimiento informático que garantiza su irreproducibilidad y confidencialidad, asignada a una persona natural o jurídica por una autoridad certificadora, y que está contenida electrónicamente en un medio físico, tal como una tarjeta inteligente u otros análogos”,⁵² es la que se utiliza para firmar digitalmente; para crear una firma digital, mientras que la clave pública es aquella que se emplea para verificar esa firma digital y se define como: el conjunto de datos únicos e inalterables generados en forma simultánea con la llave privada, que se corresponde unívocamente a los datos contenidos en ésta última, es asignada por la autoridad certificadora a la misma persona natural o jurídica titular de la llave privada, y que es mantenida en un archivo electrónico identificable con el titular.⁵³ En todo caso el conocimiento de la llave pública no permite deducir la clave secreta correspondiente.

El Foro Electrónico Jurídico Europeo en su Seminario Especial (Bochum, Alemania) dentro del XXI Congreso Internacional del Notariado Latino (Berlín, del 28 de mayo al 3 de junio de 1995)⁵⁴ estableció teóricamente la posibilidad de la certificación de firmas electrónicas dentro de la Notaría con la adquisición de un hardware del cual se obtendrían microordenadores (tarjetas en blanco) que imprimen un número con características de 123 dígitos que corresponden a lo que serían las huellas digitales. Mediante este hardware en las Notarías se daría a quien lo requiriera su clave pública de la cual se autenticaría su firma electrónica. Con dicha tarjeta la persona podría por ejemplo, suscribir contratos electrónicos, en cuyo caso el receptor acudiría al Notario Público del lugar en el que se encuentre para que éste, previa consulta al Registro de Claves Públicas, certificará la autenticidad de la firma digital y su vigencia.

⁵² Idem.

⁵³ Idem.

⁵⁴ Kemper, Ana Maria. Ob. cit..

Componentes técnicos.

Los componentes técnicos son los que deben ser implementados para dar seguridad a la firma electrónica, a saber:

- ◆ Para la generación y almacenamiento de claves de firmas y la generación y verificación de firmas digitales, se deberán utilizar componentes técnicos que tengan características seguras que hagan confiablemente detectable la falsificación de firmas digitales y la falsificación de información firmada, y que protejan contra el uso no autorizado de claves de firma privadas.
- ◆ Siendo un sistema técnicamente confiable aquel en que los equipos de computación, software y procedimientos relacionados sean razonablemente confiables para resguardar contra la posibilidad de intrusión o de uso indebido; brinden un grado razonable de disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento; sean razonablemente aptos para el desempeño de sus funciones específicas; y cumplan con los requisitos de seguridad generalmente aceptados.
- ◆ Respecto de las longitudes de claves a utilizar, se requerirá como mínimo una cantidad de bits igual o superior al doble de la longitud de claves que se puedan quebrantar al momento de generar el par de claves.
- ◆ Por su parte, la función de digesto seguro (hash function), implica una función matemática que transforma un documento digital en una secuencia de bits de longitud fija, de forma tal que: se obtiene la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo documento digital; y es computacionalmente no factible inferir o reconstruir un documento digital a partir de su digesto seguro o encontrar dos documentos digitales diferentes que produzcan el mismo digesto seguro.
- ◆ Siendo computacionalmente no factibles aquellos cálculos matemáticos asistidos por computadora que para ser llevados a cabo requieren de tiempo y recursos informáticos que superan ampliamente a los disponibles en la actualidad.

3.8. Conveniencia de la intervención notarial en la documentación electrónica.

El Notario no se encuentra relegado del proceso de informatización. Actualmente en las Notarías se utiliza comúnmente la informática en el campo de la gestión, asimismo, y aunque a futuro, se plantea la posibilidad de que vía telemática abogados y Notarios obtengan de manera inmediata información de las principales oficinas públicas, privadas y en especial de entidades prestadoras de servicios públicos.

Desde hace algunos años a nivel internacional se están estudiando los aspectos de la contratación electrónica, certificación de firmas electrónicas, y elaboración de documentos digitales en la Notaría; actividades que no excluirían la actividad actual desarrollada por el Notario tipo latino, sino que la complementarían, incitándose al Notariado a asumir un rol activo en la "Revolución Digital", al reconocer la situación actual y ofrecer alternativas viables, teniendo como importante herramienta al Derecho comparado.

La participación del Notario en la realización de documentos electrónicos deberá estar prevista y regulada legislativamente, en especial tratándose de los aspectos técnicos que darán a dicho documento certeza, seguridad, autenticidad, e inalterabilidad, para lo cual el documento digital originado ante un Notario deberá ser realizado con las medidas de seguridad explicadas en el punto 3.3. de esta investigación, y en especial con un software provisto de códigos para asegurar su inalterabilidad; los mismos códigos de seguridad deberán encontrarse en el soporte informático que corresponda al titular del documento digital, tomando primordial precaución en el momento de la transmisión para evitar que se dé la posible intromisión de terceros ajenos, conocidos como "Hackers".

Asimismo, deberá estudiarse la creación de un sistema de conservación documental electrónica notarial, y la forma de custodia y actualización del mismo. Dicha documentación quedará custodiada por el Notario, el cual garantizará su consulta permanente. Se debe permitir que las personas que lo soliciten tengan acceso a la información y puedan verificar las operaciones realizadas a través de un registro sistemático de éstas el cual hará evidente cualquier anomalía.

La aplicación de estas nuevas tecnologías al documento público se hará respetando los principios del mismo, que hacen que dicho documento sea de prueba plena en nuestro orden jurídico. Para ello, necesariamente se tendrá que requerir por parte del Notario el contar con una especialización en informática jurídica, y poseer al menos conocimientos básicos de computación.

Como ya se hizo mención en el Proyecto de Ley sobre Documento Electrónico de la República de Chile, se regula la actividad documental de este tipo con la inclusión de los Notarios Públicos en la misma, se establece que el Notario como funcionario investido de la fe pública que le ha delegado el Estado para el ejercicio de su función es, en principio, el único autorizado a elaborar y/o certificar documentos electrónicos y/o a certificar firmas digitales en aquellos documentos privados.

En dicho Proyecto se establece que las formalidades como son la escrituración, la firma, el archivo, la firma ante Notario, la escritura pública, las inscripciones en los Registros Conservatorios, y las funciones notariales de conservadores y archiveros quedan en condiciones de ser cumplidas mediante documentos electrónicos con la participación activa de los Notarios y sus asociaciones profesionales.

Pero, para que la intervención del Notario en la documentación electrónica sea una realidad se deberá dictar legislación sobre el documento electrónico, realizar acuerdos entre juristas y técnicos a fin de lograr establecer parámetros técnico/jurídicos seguros e inviolables referentes a la documentación jurídica electrónica, y efectuar ensayos piloto de conclusión de contratos por medios telemáticos.

En cuanto a la infraestructura de la firma digital el Notario podrá desarrollar actividades como las siguientes: La verificación de los datos de una persona a efectos de registrar una clave pública y obtener un certificado de la autoridad certificante; la certificación de la identidad y capacidad de una persona con el objeto de realizar una operación; la

verificación de todos los aspectos formales y legales relacionados con la transacción en sí, como punto fundamental de la función notarial; la certificación de copias en soporte digital de documentos originalmente expedidos en otro soporte, mediante la aplicación de la firma digital del Notario; certificación de firmas digitales; expedición del testimonio con la firma digital del Notario; y actuación como depositario de la clave privada en los casos en que corresponda; además de las que le corresponderían como Autoridad Certificante Licenciada.

En cuanto a la formalización de contratos electrónicos ante Notario, está podrá darse:

Entre presentes con la comparecencia de ambas partes contratantes, o entre ausentes (vía telemática) con la intervención de dos Notarios uno en cada demarcación: el primero donde se realice el documento y el segundo donde se reciba.

3.8.1. El Proyecto del Cibernotario.

Es un Proyecto desarrollado en Estados Unidos patrocinado por el Cybernotary Comitee de la American Bar Association (Comité del Cibernotario de la Asociación de la Barra Americana), con el propósito de que sea implementado como complemento de la infraestructura de la firma digital.

Este Proyecto surgió debido a que con el incremento del comercio electrónico internacional también se acrecentó el problema de la aceptación de aquellos actos creados en los Estados Unidos para ser utilizados fuera o con efectos en otros países, rechazándose muchos de ellos principalmente en los países que pertenecen a la familia romano-germánica como es el caso de México. En un inicio trató de darse solución al problema brindando asesoría legal norteamericana a aquéllos que fueran a realizar alguno de los actos antes mencionados, pero ello no fue la solución idónea; el abogado norteamericano podía no estar asegurado contra la eventual responsabilidad que esto acarrearía, implicaba altos costos para los interesados, y el abogado estadounidense únicamente emitía una carta-opinión no satisfaciendo los requisitos de otros países que solicitan que para determinados actos intervenga una tercera parte no interesada. Por ello, el Proyecto surgió con la esperanza de que se garantice a estos documentos su aceptación en cualquier jurisdicción (local o extranjera).

Este Proyecto prevé la creación de una oficina cuasi-pública o Cibernotario que ejercerá dos funciones complementarias:

a) La práctica notarial internacional. En este contexto su función será similar a la que normalmente realiza un Notario, pero será un abogado del common law realizando funciones semejantes a las de un Notario tipo latino, constituyendo un puente entre las dos tradiciones surgiendo un acto que reúna los requisitos de procedimiento y formalidades necesarios en ambos sistemas. Con ello se espera que los actos pasados ante el Cibernotario tengan pleno reconocimiento y efectos fuera de Estados Unidos; y

b) La práctica notarial electrónica. El abogado será un profesional con alto nivel de especialización en seguridad tecnológica, lo que le permite tener capacidad de certificación y autenticación electrónicas en una transacción comercial digital. El Cibernetario utilizará la firma electrónica para certificar la identidad del emisor del mensaje; fechará electrónicamente la fecha y hora de su intervención y protocolizará con fines de archivo; intervendrá en las transacciones de Derecho comercial internacional; determinará la capacidad del firmante (identificará a la persona y en caso necesario investigará sus antecedentes); verificará todos los aspectos relacionados con la transacción; y verá que se cumplan con los requisitos de fondo y forma de la jurisdicción que corresponda, es decir dará seguridad en dichas transacciones.

3.9. El documento electrónico como medio de prueba.

Hoy en día numerosas actividades son llevadas a cabo por medios electrónicos sin tener el suficiente apoyo legal, al no existir los suficientes ordenamientos jurídicos específicos que regulen a estos soportes, lo que hace necesaria la actualización constante de estos textos para adecuarlos al fenómeno informático.

En el caso del documento electrónico como medio de prueba se considera difícil el encontrar un punto de apoyo que justifique la negación de éste supuesto, especialmente porque el ser humano se desenvuelve en una sociedad tecnológica y requiere del reconocimiento de medios probatorios digitales para su correcta defensa. Debiéndose aceptar el documento electrónico como un medio de prueba admisible, especialmente en caso de ausencia de consagración expresa en el ordenamiento jurídico, ya que el fenómeno informático ocasionó la necesidad de una nueva concepción ante los escritos en forma tradicional.

Así, si bien en muchas legislaciones de carácter probatorio aún no se recogen expresamente las técnicas electrónicas, la tendencia actual es la de admitir al documento electrónico como medio de prueba y reconocerle igual valor probatorio que al documento escrito; aunque algunos hacen depender dicho valor con base a la libre convención de las partes, o simplemente (la mayoría) permiten al juez amplia libertad para decidir sobre su valor.

De esta forma, países como Gran Bretaña (Ley de Evidencia Civil de 1968, sección 5a. consagrada a la informática) y Australia (Ley de Enmienda sobre la Evidencia Australiana de 1972, sección 14), ya prevén el fenómeno informático; y la última considera a la informática como un derecho de prueba eficaz. Por su parte, en España en el Código Civil dentro de los medios de prueba se permite considerar al documento informático (electrónico o impreso) con pleno valor probatorio, siempre que existan los medios técnicos para comprobar su integridad y autenticidad.⁵⁵

En nuestro país, la prueba en sentido estricto es la obtención de cercioramiento del juzgador acerca de los hechos discutidos y discutibles, cuyo esclarecimiento resulte

⁵⁵ Idem.

necesario para la resolución del conflicto sometido a proceso. En sentido amplio, comprende todas las actividades procesales que se realizan a fin de obtener dicho cercioramiento, se obtenga éste o no.⁵⁶

Siendo los medios de prueba los instrumentos con los que se pretende lograr el cercioramiento del juzgador acerca de los hechos discutidos en el proceso, sobre los hechos objeto de prueba. Estos instrumentos pueden ser objetos materiales -documentos, fotografías, etcétera- o conductas humanas realizadas bajo ciertas condiciones. Con los avances tecnológicos actuales la mayoría de los medios de prueba pueden interrelacionarse con las computadoras, pero son las pruebas documentales las que guardan mayor relación debido al documento electrónico.

Con las reformas publicadas el 10 de enero de 1986, se modificó el artículo 289 del CPCDF para establecer de forma genérica que "son admisibles como medios de prueba aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos".

Con respecto a los medios de prueba adquiere importante significado el sistema de apreciación probatoria, al ser la operación exteriorizada en la sentencia a través de la cual el juzgador determina la fuerza probatoria de cada uno de los medios de prueba.

Existiendo diversos sistemas de valoración probatoria, a saber:

1.- *El legal o tasado.* En este sistema la Ley establece los medios de prueba, y la valoración que debe darles el juez, o sea que los medios de prueba tienen un valor o tasa inalterable y constante establecido apriorísticamente y a los que el juzgador debe sujetarse. El juez deberá limitarse a revisar si las pruebas se practicaron de conformidad con las exigencias legales, por lo que en este sistema se priva al juzgador de cualquier intervención subjetiva para determinar la valoración.

Así, para que el documento electrónico sea considerado como un medio de prueba en este sistema, dicho documento deberá ser considerado expresamente como tal en la Ley.

2.- *El de libre apreciación razonada o sana crítica.* En el sistema de sana crítica no existen reglas apriorísticas a las que se encuentre sometido el juzgador, por lo que puede apreciar y otorgar valor probatorio de forma libre, siempre que se sujete a reglas de coherencia lógica y funde, y motive su resolución.

3.- *El sistema mixto.* Dicho sistema es una mezcla de los dos anteriores, por lo que en algunos casos la Ley sujeta al juzgador a valores previamente establecidos en la misma, pero deja otros más al libre criterio del juez.

4.- *El de íntima convicción. o libre convicción.* Este sistema es propio de los jurados populares, y no es aplicable en materia civil, en él se permite mayor discrecionalidad al juez, quien es libre de decidir y no tienen necesidad de justificar la razón de su decisión.

⁵⁶ Ovalle Favela, José. Ob. cit., pág. 107.

En los últimos sistemas descritos no existirá obstáculo alguno para la admisión de los documentos electrónicos como medios de prueba y el juez podrá otorgarles el valor que crea conveniente, siempre que no exista norma que se lo prohíba expresamente.

En el CPCDF antes de las reformas de 1986, el sistema regulado era el mixto, pero a partir de esas reformas se estableció el sistema de la sana crítica en los artículos 402 y 403 del propio ordenamiento legal. De acuerdo con el artículo 402, los medios de prueba aportados y admitidos, serán valorados en su conjunto por el juzgado, atendiendo a las reglas de la lógica y de la experiencia; en todo caso, el tribunal deberá exponer cuidadosamente los fundamentos de la valoración jurídica realizada y de su decisión. El artículo 403 excluye del sistema de la libre valoración razonada a los documentos públicos, a los que se confiere valor probatorio pleno.

El artículo 402 plantea un problema interpretativo al no establecer que se deberá entender por reglas de la lógica y de la experiencia, lo que no deberá quedar al arbitrio del juez, sino ser determinado por la jurisprudencia; siendo éste también un campo fértil para la doctrina. La doctrina chilena al respecto considera que el juez debe asesorarse por sus conocimientos técnicos, su experiencia personal, la lógica, el sentido común, el buen juicio y la recta intención.⁵⁷

En el caso específico del documento electrónico será más fácil probar con base en él si se toman ciertas precauciones técnicas como las enunciadas en el punto 3.3. de esta investigación, entre otras la elección de determinados sistemas de cómputo seguros, el uso de un CD-WORM (Write Once Read Many); si el documento electrónico se transmite por medios telemáticos como Internet se debe procurar el uso de un formato de edición especial, el formato de documento portátil (PDF), y la utilización de medios de autenticación técnicamente confiables, aunque ello implique gastos adicionales otorgará seguridad. De la misma forma para obtener esa seguridad, antes de realizar cualquier acto jurídico respaldado por un documento digital se debe tener certeza de que servirá como medio probatorio, ya que en caso contrario se deberá optar por las formas tradicionales como el soporte en papel y firmas autógrafas.

Así, en el CPCDF no existe impedimento legal para la admisión de documentos electrónicos como medios de prueba, y se considera como único obstáculo real para la valoración de los documentos digitales, el que el juez no posea los conocimientos técnicos necesarios para llevarla a cabo. Desgraciadamente, en el CPCDF no se hace mención a los documentos electrónicos como tales (situación que no se puede postergar). Por otra parte, resulta importante hacer mención a que en la Ley del Mercado de Valores en sus capítulos relativos al contrato de intermediación bursátil e informatización si se prevé al documento electrónico como medio de prueba.

⁵⁷ Herrera Bravo, Rodolfo. Ob. cit..

CAPÍTULO

IV

LA CONTRATACIÓN ELECTRÓNICA.

La importancia práctica de la contratación electrónica se maximiza con la implementación de medios telemáticos, especialmente de Internet. Como se recordará la Red comenzó a usarse con fines de investigación, para con el paso del tiempo abarcar a las transacciones comerciales; en éste momento se inició a prestar atención al contrato electrónico como soporte de las transacciones comerciales, y actualmente el uso y eficacia del Internet se ha extendido hasta abarcar una mayor cantidad de contratos de las más diversas materias, incrementándose la necesidad de conocer las implicaciones jurídicas de este fenómeno en el aspecto contractual.

En este momento los principales medios que se usan para realizar contratos digitales son el correo electrónico, y el World Wide Web; donde el documento informático trae aparejadas importantes consecuencias, entre ellas la de una nueva forma de contratar sobre las ya existentes, a las que se sumaría la electrónica, siendo esencial establecer que el documento electrónico implica el uso de un nuevo soporte pero no altera el contenido jurídico de los actos. En contra de la implementación del documento electrónico se esbozaron importantes dificultades como fueron el asegurar la inalterabilidad del acto contenido en el documento, la identificación fehaciente de los contratantes y el correcto funcionamiento de la firma digital; dificultades actualmente superadas en su mayoría gracias a la propia tecnología y a soluciones propiamente jurídicas.

De esta manera hoy en día, diversas legislaciones ya han iniciado el establecimiento de la contratación electrónica en el ordenamiento jurídico. Así, en la XXIV Jornada Notarial Argentina (Buenos Aires, octubre de 1996)¹ se declaró que el documento electrónico es válido y eficaz como forma de contratación, y en el Proyecto de Ley sobre Documentos Electrónicos de la República de Chile se estableció el Título III consagrado a los Contratos de Intercambio de Documentos Electrónicos.²

4.1. La etapa precontractual.

La mayor parte de los contratos antes de perfeccionarse cruzan por una serie de gestiones precontractuales, que permiten a las partes obtener finalmente un acuerdo en favor del cual expresan su consentimiento.

¹ XXIV Jornada Notarial Argentina, Buenos Aires, octubre de 1996. Ob. cit..

² Proyecto de Ley sobre Documentos Electrónicos de la República de Chile. Ob. cit..

La trascendencia de la fase preparatoria es especialmente importante en la contratación electrónica dada la volatilidad de los medios telemáticos que son, por excelencia aquéllos que las partes usan para transmitir sus comunicaciones.

En los contratos electrónicos resulta esencial que las partes se informen de los riesgos (pueden incluso desear asesoría de expertos en la materia) que implica la utilización de este sistema, en el que la manera de exteriorizar la voluntad es a través de documentos electrónicos, resultando esencial poder constatar la identidad de las partes y la integridad de las manifestaciones de voluntad para que el contrato por Internet tenga eficacia. Como ya se ha mencionado, para demostrar la identidad se puede usar, por ejemplo la firma digital o la intervención de terceras partes confiables y en cuanto a la integridad, principalmente se implementa la criptografía y el uso de canales seguros de comunicación. Asimismo, las partes deberán evaluar cuidadosamente aspectos como la clase de bien o servicio que desea recibir, los costos, la eficiencia, y la seguridad entre otros.

Afortunadamente, en nuestros días los avances tecnológicos brindan la seguridad necesaria para que la legislación pueda reconocer a los documentos electrónicos, y a la contratación electrónica de la misma manera en que se reconoce a los documentos y contratos tradicionales.

4.2. El contrato electrónico.

El artículo 1793 del Código Civil para el Distrito Federal establece que los convenios que producen o transfieren las obligaciones y derechos toman el nombre de contratos.

Siendo la contratación electrónica aquella que utiliza como medio o herramienta para transmitir declaraciones de voluntad de las partes contratantes la comunicación informática o telemática, independientemente de que el objeto de la contratación sea informático o no; siendo una de sus características el que la información enviada y recibida no está soportada en papel.³

El Dr. Jaime Tomas Guerra Balic refiriéndose al contrato electrónico hace consideraciones especiales en cuanto a los elementos que intervienen en la elaboración del documento electrónico. El considera jurídicamente al hardware como todo tipo de aparato capaz de procesar electrónicamente información y transmitir un mensaje; cuyos efectos tengan una trascendencia jurídica de carácter contractual. Y señala que, en el caso de los contratos el software reviste especial importancia, ya que en él se especifica un conjunto de reglas que servirán de marco general a la celebración del contrato haciendo uso de un ordenador para exteriorizarlas. Cuando dicho conjunto de reglas es ejecutado surge una nueva relación contractual diferente a la anterior.

En este orden de ideas, para que la relación contractual pueda realizarse a través de una computadora deberá satisfacer las características básicas de que exista acuerdo previo

³ Carvajal Higuera, Luis Alfonso. "OBEC'97 Overcoming Barriers to Electronic Commerce -Superando las Barreras hacia el Comercio Electrónico-". Disponible [Online]:<<http://emn.derecho.uma.es/obec/abstracts/ab333Carvajal.htm>>

respecto al programa que va a ser utilizado, que se acepte dicho programa, y que el soporte del contrato resultante no sea un documento escrito en papel. Dicho software deberá ser creado por una persona idónea con el fin de obtener una documentación electrónica segura.⁴

Por su parte, el Proyecto sobre Documentos Electrónicos de la República de Chile en el Título III regula los contratos de intercambio de documentos electrónicos. En este Título, en general, se establecen disposiciones que suplen la voluntad de las partes en los contratos (escritos o no), que traten sobre la generación, comunicación, recepción, archivo o cualquier otro acto de procesamiento de documentos electrónicos. Sin embargo, estas disposiciones podrán ser modificadas por acuerdo de las partes cuando la ley no se oponga a ello (artículo 14).⁵

4.2.1. La autonomía de la voluntad.

El principio de la autonomía de la voluntad es la base del Derecho en materia contractual, implica que la voluntad de las partes contratantes es libre, por lo que podrán incluir en el contrato el contenido y las cláusulas que deseen; pueden pactar todo aquello conveniente a sus intereses siempre que no esté legalmente prohibido.

En el caso de la contratación electrónica, su elección deberá surgir de la libre voluntad de las partes, las cuales deberán acordar el hardware y el software a utilizar, así como todos los aspectos necesarios para que se obtenga una documentación electrónica segura y conforme a la manifestación de voluntad por ellas exteriorizada.

En nuestro país, actualmente diversas compañías establecen un contrato previo a aquél que se pretende realizar por medios telemáticos, donde se señalan las cláusulas por ellas acordadas en cuanto a la contratación electrónica. Esta práctica, por seguridad legal se está implementando en diversos países, pero por desgracia aumenta los costos y resulta impráctica, por lo que sólo la utilizan aquéllos que con frecuencia usan este sistema para contratar.

4.2.2. El consentimiento.

El consentimiento es un elemento esencial del contrato que consiste en el acuerdo de dos o más voluntades sobre la producción o transmisión de obligaciones y derechos, siendo necesario que estas voluntades tengan manifestación exterior,⁶ y que se realice en los términos de una norma para la producción de las consecuencias previstas en la misma.⁷

Las voluntades debe manifestarse, deben rebasar la interioridad donde se crean para tener existencia social y jurídica, y para ello se expresan por cualquier forma de

⁴ Kemper, Ana María. Ob. cit.

⁵ Proyecto de Ley sobre Documentos Electrónicos de la República de Chile. Ob. cit.

⁶ Borja Soriano, Manuel. "Teoría General de las Obligaciones". Porrúa, 13a. edición, México, 1994, pág. 121.

⁷ Zamora y Valencia, Miguel Angel. "Contratos Civiles". Porrúa, quinta edición, México, 1994, pág. 28.

comunicación, pudiendo perfectamente exteriorizarse por medios telemáticos o informáticos e integrar el consentimiento.

Para que se integre el consentimiento se requiere la coincidencia de la oferta de una de las partes contratantes y la aceptación de la otra. En el caso de los contratos electrónicos, a pesar de que se pueden realizar contratos entre presentes, los que poseen mayor trascendencia económica y práctica son aquéllos que se realizan entre ausentes o a distancia, a través de medios telemáticos. En este caso, habrán de retomarse los postulados jurídicos ya aceptados con respecto a la contratación entre ausentes, debido a que los principios son los mismos, lo único novedoso, en este caso es el medio de transmisión.

Sin embargo, al igual que el documento electrónico, la contratación electrónica entre ausentes debe superar problemas técnicos, como la pérdida del mensaje por un error en la dirección a la que se envía o por una falla en la transmisión del ordenador, entre otras causas; para lo que, tanto las partes como los proveedores de acceso deberán mantener registros sistemáticos inalterables y perdurables de los mensajes enviados y transmitidos. En el caso de Internet, el consentimiento podrá perfeccionarse vía correo electrónico o World Wide Web. A través del correo electrónico el oferente podrá enviar la oferta y recibir la respuesta como si se tratará de correspondencia, sólo que en algunos casos el tiempo de espera será mucho menor al del correo habitual. Mientras que el World Wide Web⁸ permite una transmisión de datos mucho más rápida que el anterior.

4.2.2.1. La oferta y la aceptación.

La oferta o policitación consiste en la propuesta de las condiciones de un contrato que hace uno de los futuros contratantes al otro, siendo la aceptación la conformidad que el otro contratante manifiesta con respecto a la propuesta, quedando formado el consentimiento.⁹ Así, y de conformidad con el artículo 1807 del Código Civil el contrato se forma en el momento en que el proponente reciba la aceptación.

En los contratos entre presentes la aceptación debe darse de inmediato o el ofertante queda desligado de la oferta, a menos que haya señalado plazo para aceptarla; en caso de que se haya fijado un plazo, el ofertante quedará ligado a su oferta hasta la expiración del plazo. Tratándose de la oferta hecha por teléfono se aplicarán las normas relativas al contrato entre presentes (artículos 1804 y 1805 del Código Civil).

⁸ La mayor parte de los contratos celebrados en el World Wide Web son contratos de adhesión. Éstos contratos implican un desequilibrio entre los contratantes, por lo que los sistemas legales protegen al consumidor. Así, son definidos en el artículo 85 de la Ley Federal de Protección al Consumidor como "el documento elaborado unilateralmente por el proveedor, para establecer en formatos uniformes los términos y condiciones aplicables a la adquisición de un producto o a la prestación de un servicio, aún cuando dicho documento no contenga todas las cláusulas ordinarias de un contrato. Todo contrato de adhesión celebrado en territorio nacional, para su validez, deberá estar escrito en idioma español y sus caracteres tendrán que ser legibles a simple vista".

⁹ Borja Soriano, Manuel. Ob. cit., pág. 121.

El contrato entre presentes es aquel que se celebra estando los contratantes uno en presencia del otro o al menos en las mismas condiciones que si se encontraran en el mismo lugar, pudiendo de forma directa negociar el contrato.

Por su parte, el contrato entre ausentes es aquel en que dicha comunicación entre los contratantes no puede darse de forma directa; por ello, los contratos entre ausentes revisten más complicaciones que aquéllos celebrados entre presentes. Situación que genera que nuestro Código Civil en cuanto a éstos contratos prevea diversos supuestos, entre ellos: la aceptación modificando la propuesta, en cuyo caso el proponente quedará libre de su oferta y la respuesta se considerará como una nueva proposición (artículo 1810); el fallecimiento del proponente al tiempo de la aceptación, sin que el aceptante fuere sabedor de su muerte, situación en la que quedarán los herederos de aquél obligados a sostener el contrato (artículo 1809); el caso en que el autor de la oferta la retire, supuesto en el cual la oferta se considerará como no hecha, si la retira su autor y el destinatario recibe la retractación antes que la oferta -la misma regla se aplica en el caso de que se retire la aceptación- (artículo 1808); y la oferta y aceptación hecha por telégrafo, circunstancia en la que éstas producirán efectos si los contratantes con anterioridad habían estipulado por escrito esta manera de contratar y si los originales de los respectivos telegramas contienen las firmas de los contratantes y los signos convencionales establecidos entre ellos (artículo 1811).

Pero en los contratos entre ausentes resulta especialmente importante determinar por cuanto tiempo la oferta hecha se mantiene vigente y cual es el momento en que el consentimiento queda plenamente integrado. En cuanto a la primera situación a considerar, nuestra legislación civil indica que la oferta se mantendrá vigente si se fijó plazo hasta la expiración de éste (artículo 1804 del Código Civil); y en caso de que la oferta se haya hecho sin fijación de plazo para aceptarla, el oferente quedará ligado durante tres días, además del tiempo necesario para la ida y vuelta regular del correo público, o del que se juzgue bastante, no habiendo correo público, según las distancias y la facilidad o dificultad de las comunicaciones (artículo 1806 del ordenamiento legal antes citado).

En cuanto, al momento en que el consentimiento queda integrado doctrinalmente se reconocen cuatro sistemas para determinarlo:

- ◆ Sistema de la declaración. El consentimiento se integra en el momento en que la aceptación se manifiesta independientemente de la manera en que se dé, no existiendo necesidad de hacer saber al oferente dicha aceptación. Este sistema acarrea diversas dificultades en materia de prueba.
- ◆ Sistema de la expedición. El consentimiento se forma cuando la aceptación, además de manifestarse, se remite al oferente. Considerándose que esa remisión se da cuando la aceptación sale del dominio absoluto de aceptante.
- ◆ Sistema de la recepción. El consentimiento se estructura cuando el documento que contiene la aceptación es recibido por el oferente, se entere éste o no del contenido de dicho documento. Gracias a que la recepción es un hecho material se facilita su prueba.
- ◆ Sistema de la información. El consentimiento se integra cuando además de que el oferente ha recibido la aceptación ésta se ha hecho de su conocimiento.

En el caso del Código Civil, el sistema adoptado para la integración del consentimiento, y por tanto para la formación del contrato es el de la recepción; el artículo 1807 establece que "El contrato se forma en el momento en que el proponente reciba la aceptación, estando ligado por su oferta según los artículos precedentes".¹⁰

De la misma forma, en cuanto a contratación electrónica se adopta el sistema de la recepción en el Proyecto de Ley sobre Documentos Electrónicos de la República de Chile¹¹, prescribiendo que en cuanto a la formación de contratos, todo acto jurídico podrá ser otorgado o celebrado mediante documentos electrónicos, por lo que cuando en la formación de un contrato se utilicen documentos electrónicos, no podrá negarse la validez o la exigibilidad del contrato, por la sola circunstancia de que se utilizaron documentos electrónicos para dicho efecto. Y agrega que la formación del consentimiento en los actos jurídicos se producirá cuando el originador reciba la aceptación del destinatario, mediante el envío del correspondiente mensaje o documento electrónico, siendo el originador aquel que firma digitalmente un documento y lo envía (situaciones reguladas en los artículos 23 y 15 que no pueden ser modificados por las partes).

Por su parte, el Proyecto de Ley No. 227 de Colombia¹² indica que en la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresados por medio de un mensaje de datos el cual tendrá todos los efectos jurídicos, la validez y fuerza obligatoria de un contrato. Y en todos los casos, las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje.

En diferentes proyectos referentes a los documentos electrónicos, salvo acuerdo en contrario, se establecen normas similares aplicables al acreditamiento de la integridad, la autenticidad, y el momento de la recepción del documento electrónico. De conformidad con ellos, en cuanto a los elementos de autenticación e integridad de un documento electrónico, éstos se entenderán cumplidos si se aplicaron de forma apropiada los procedimientos adecuados, ya sea porque se hayan acordado previamente entre las partes, o sean razonables de acuerdo a las circunstancias, tales como las relaciones existentes entre las partes, los documentos intercambiados con anterioridad, la existencia de un contrato, etcétera; y siempre que el receptor del documento haya adoptado las precauciones razonables o aplicado el procedimiento previamente convenido. Además, se podrá solicitar un acuse de recibo el cual implica que se ha cumplido con la recepción, e incluso con la integridad y la autenticidad, si en el mismo se especifica que se recibió el mensaje de datos conforme a ciertos requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable.

¹⁰ En materia mercantil el sistema adoptado es el de la expedición, excepto en algunos casos en materia internacional: México suscribió en abril de 1980 la Convención de Viena sobre la Venta Internacional de Mercaderías, aplicable a los medios telemáticos y de conformidad con la cual en materia de compra-venta internacional se adopta la teoría de la recepción. Esta Convención sólo compromete a los países firmantes. Barrios Garrido, Gabriela; et al. Ob. cit., pág. 70. Por su parte, el Proyecto de Ley sobre Documentos Electrónicos de la República de Chile, establece que se entiende que el envío del documento electrónico tiene lugar cuando el documento entra en un sistema de información que está fuera del control de aquél que lo envía.

¹¹ Proyecto de Ley sobre Documentos Electrónicos de la República de Chile. Ob. cit..

¹² Proyecto de Ley No. 227 de Colombia. Ob. cit..

Y en cuanto al momento de recepción del documento electrónico, las reglas generales aplicables son que si se ha indicado el sistema de información que deberá recibir el documento digital, se entiende que la recepción del mismo se da en el momento en que el documento entra en dicho sistema de información, pero si no se ha indicado un sistema de información en específico, se entenderá recibido en el momento en que el documento entre en cualquier sistema de información de la persona a la cual se le envía.

4.2.3. El objeto.

El objeto es un elemento esencial del contrato, como lo indica el artículo 1794 del Código Civil al asegurar que “para la existencia del contrato se requiere...II. Objeto que pueda ser materia del contrato”.

Doctrinalmente el objeto directo del contrato es la creación o transmisión de derechos y obligaciones, siendo el objeto de las obligaciones y el indirecto o mediato del contrato una prestación positiva (dar -dar una cosa-, o hacer -un hecho a ejecutar por el deudor-) o negativa (no hacer); también el hecho y la cosa misma son objetos del contrato.

Estableciendo el ordenamiento legal antes citado que son objeto de los contratos: La cosa que el obligado debe dar, y el hecho que el obligado debe hacer o no hacer (artículo 1824); la cosa objeto del contrato debe existir en la naturaleza, ser determinada o determinable en cuanto a su especie y estar dentro del comercio (artículo 1825); y el hecho positivo o negativo de un contrato debe ser posible y lícito (artículo 1827).

Tratándose de la contratación electrónica, no debe confundirse el contrato electrónico con el contrato informático. Los contratos informáticos surgieron debido al contenido altamente técnico de los mismos y a la evidente desigualdad entre las partes ocasionada por la cantidad y cualidad de conocimientos atesorados por el proveedor (aquella parte de la relación contractual encargada de proporcionar un bien o servicio informático) en desventaja del usuario. Por lo que, en cuanto al objeto del contrato, los contratos electrónicos podrán tener cualquier objeto permitido por la Ley, mientras que en los contratos informáticos el objeto recae sobre bienes (por ejemplo, el hardware) o servicios informáticos necesariamente (como la asistencia técnica o el mantenimiento del software).

4.2.4. La forma.

El Derecho desde tiempos inmemoriales ha exigido una forma para perpetuar los actos jurídicos trascendentes, permitiendo que dichos actos sean mantenidos en el tiempo y conocidos por aquéllos a quienes afectan o interesan. Hasta hace poco, el soporte en papel y la escritura eran ideales para cumplir esos fines. Sin embargo, en la actualidad un contrato plasmado en papel mediante la escritura y con una firma ológrafa simplemente no es concebible en los medios telemáticos; por costo, velocidad y eficiencia se evita en lo posible el documento tradicional, y en algunas esferas incluso se considera como anticuado.

La forma en general, es la manera de exteriorizar el consentimiento en el contrato y comprende todos los signos sensibles (lenguaje -verbal, escrito, o mímica-), las personas antes quienes se debe expresar, los archivos en que debe constar, y determinadas menciones que deben hacerse (que las partes convienen o la ley establece para lograr esa exteriorización).¹³

Dicho consentimiento puede exteriorizarse con manifestaciones directas (verbal, escrito, o por signos inequívocos), en cuyo caso se le considera como consentimiento expreso; o por medio de manifestaciones indirectas (hechos o actos que lo presupongan o autoricen a presumirlo), denominándose consentimiento tácito (artículo 1803 del Código Civil).¹⁴

Nuestro Código Civil en el artículo 1832 establece que "En los contratos civiles cada uno se obliga en la manera y términos que aparezca que quiso obligarse, sin que para la validez del contrato se requieran formalidades determinadas, fuera de los casos expresamente designados por la ley", y en el artículo 1796 indica que "Los contratos se perfeccionan por el mero consentimiento, excepto aquéllos que deban revestir una forma establecida por la ley. Desde que se perfeccionan obligan a los contratantes..."; disposiciones que nos permiten afirmar que en nuestro Derecho, los contratos en principio son consensuales (pudiendo las partes adoptar libremente la forma de exteriorización del consentimiento que prefieran), limitados por las excepciones establecidas en la ley.¹⁵ Así, aplicando el principio de libertad de formas puede aceptarse el soporte informático.

En el caso de que la ley establezca una forma determinada se aplica el artículo 1834 del ordenamiento legal antes citado, el cual señala que "Cuando se exija la forma escrita para el contrato, los documentos relativos deben estar firmados por todas las personas a las cuales se les imponga esa obligación. Si alguna de ellas no puede o no sabe firmar, lo hará otra a su ruego y en el documento se imprimirá la huella digital del interesado que no firmó".

"Cuando el legislador habla de escritura, quiere referirse a la noción común de ésta",¹⁶ y conforme a esta noción como ya se demostró en el punto 3.1. no hay problema alguno para que el documento electrónico asuma el valor de acto escrito. En lo referente a la firma, ésta se define como el "Nombre y apellido (o apellidos) que una persona pone, con rúbrica o sin ella, al pie de un escrito como señal de autenticidad",¹⁷ por lo que tampoco se encuentra

¹³ Zamora y Valencia, Miguel Angel. Ob. cit., pág. 31.

¹⁴ El consentimiento exteriorizado por medios telemáticos puede ser tanto expreso como tácito e incluso verbal, ya que existen los medios tecnológicos para efectuarlo.

¹⁵ De conformidad con el Código de Comercio en las convenciones mercantiles cada uno se obliga en la manera y términos que aparezca que quiso obligarse, sin que la validez del acto comercial dependa de la observancia de formalidades o requisitos determinados. Excepto aquellos que conforme a este Código o a leyes como las de ferrocarriles, minas, etcétera, requieran reducirse a escritura o requieran formas o solemnidades necesarias para su eficacia; y los contratos celebrados en país extranjero en que la ley exige escrituras, formas o solemnidades determinadas para su validez, aunque no las exija la ley mexicana. Artículos 78 y 79 del Código de Comercio comentados por Jacinto Pallares citado por Borja Soriano, Manuel, Ob. cit., p.p. 195 y 196.

¹⁶ Ettore Giannantonio. "Informática y Derecho". Ob. cit., pág. 110.

¹⁷ Pina, de Rafael; Pina Vara, de Rafael. Ob. cit., pág. 292.

dificultad para que en los documentos informáticos se acepte la firma electrónica, la cual cumple con todas las funciones de una firma autógrafa e incluso puede llegar a brindar mayor seguridad que ésta.¹⁸

La operación práctica de la firma digital sería la siguiente: "Una parte podría entonces presentar la aceptación encriptada de la otra parte, ya descryptada utilizando la clave pública, como evidencia computarizada de un contrato cerrado por Internet. Esta operación inequívoca prueba la identidad y el consentimiento de la segunda parte. Déjenos considerar un caso en el que la parte A envía a la parte B un contrato para que lo firme. B teclea una fórmula de consentimiento y después indica su aprobación al contrato como un todo encriptándolo mediante su clave privada. Como la única forma de descryptar esta aceptación es utilizando la clave pública de B, es claro que la aceptación solo pudo encriptarse usando la clave privada de B. Entonces, A posee la prueba adecuada de la expresión del consentimiento de B".¹⁹

Respecto a los documentos electrónicos también es importante determinar cuando se consideran como un documento original, y cuando como un documento fechado, a saber:

Las legislaciones y proyectos que han tratado el tema de los documentos electrónicos, han considerado como originales a todos los documentos digitales íntegros, evitando fórmulas complicadas. Sin embargo, el autor Olivier Hance propone un sistema propio para determinar la originalidad del documento electrónico.

Él parte de la premisa de que la originalidad del documento con soporte papel tradicionalmente se demuestra con la firma, ya que en una copia la firma será también una copia, mientras que un original tanto la firma como el documento son originales. Y agrega que en un documento electrónico lo anterior es difícil de determinar debido a que la copia digital es idéntica a su matriz, lo cual no implica la existencia de dos originales, por lo que para que se asegure la originalidad de los documentos electrónicos el autor da como solución que al igual que en los documentos con soporte papel en donde cada firma se plasma en diferente lugar, en los documentos electrónicos la encriptación y la firma electrónica se realicen en diferente secuencia. "Entonces ¿cuál es la solución para probar que pueden producirse tantos originales como partes haya en el contrato celebrado por Internet? Las partes contratantes sólo deben "firmar" los varios originales utilizando sus respectivas claves de encriptación privadas, pero en un orden diferente en cada original...

¹⁸ En el artículo 13 de la Ley Modelo sobre Comercio Electrónico de la CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) se encuentra lo relativo a la atribución de los mensajes mediante métodos de autenticación, los cuales identifican al autor del mensaje y verifican su contenido, siempre y cuando exista un convenio previo entre las partes que establezca este método de autenticación. Así, ésta ley reconoce sólo los métodos de autenticación que fueron convenidos de manera previa por las partes, por lo que no establece el valor legal de los procedimientos, que aunque pudiesen considerarse razonables conforme a los estándares de la práctica y la técnica, no han sido aceptados por quien hizo la oferta. Barrios Garrido, Gabriela; et al. Ob. cit., p.p. 67 y 68.

¹⁹ Hance, Olivier. "Leyes y Negocios en Internet". Traducción de Yazmín Juárez Parra. McGraw-Hill, México, 1996, pág. 232.

Si el juez siempre debe utilizar las mismas claves de descriptación, pero en diferente orden, también puede, entonces, estar seguro de que ésta en presencia de originales solamente".²⁰

También en las normas federales de prueba -Federal Rules of Evidence- de los Estados Unidos se va más allá, estableciendo que un documento impreso que sea una reproducción fiel de información electrónica constituye un original.²¹

Por su parte, en el Proyecto de Ley sobre Documentos Electrónicos de la República de Chile²² se indica que esta ley se aplicará a los actos jurídicos que se otorguen o celebren a través de cualquier intercambio electrónico de datos que de como consecuencia originen documentos electrónicos (artículo 1º). Y se establece que si para cualquier efecto legal se exige que una información deba constar por escrito, estar firmada o deba ser presentada por escrito, o bien se prevén consecuencias jurídicas en el caso de que la información no conste por escrito o no este firmada, se entenderá que un documento electrónico cumple con:

- * El requisito de la escrituración, si la información contenida en el mismo es legible, está íntegra y se halla disponible para ser presentada a solicitud en cualquier momento.

- * El requisito de la firma si se ha utilizado un método o procedimiento que permita lograr la autenticación (origen y aprobación de contenido), y que el método o procedimiento utilizado sea confiable y apropiado para los fines para los cuales se generó o envió el documento electrónico, considerando todas las circunstancias aplicables al caso, incluyendo los acuerdos que puedan existir entre las partes (artículos 2º y 3º).

En el mismo Proyecto, en cuanto al requisito de originalidad se manifiesta de igual forma que si para cualquier efecto legal se exige que una información sea presentada o archivada en su forma original, o se prevé la existencia de consecuencias jurídicas para el evento de que no lo sea, se entenderá que un documento electrónico cumple con dicha exigencia si:

Existe una razonable seguridad de que la información se ha mantenido íntegra. Para determinar la integridad se deben calificar las siguientes condiciones: si la información ha permanecido completa e inalterada con exclusión de aquellos cambios que sean necesarios a consecuencia de la comunicación, archivo, recuperación o presentación de la información; si la información ha sido mantenida con niveles de seguridad acordes con los propósitos para los cuales la información fue generada y con las circunstancias del caso; y si la información puede ser presentada a la persona pertinente si ello es requerido (artículo 5º).

En cuanto al requisito de archivo, si para cualquier efecto legal se exige que ciertos documentos, registro, datos o información sean mantenidos archivados, se entenderá que se cumple con dicha exigencia si se satisfacen los siguientes requisitos copulativos:

Que la información sea accesible y esté disponible de manera que pueda ser utilizada en todo momento; si la información se ha mantenido en el formato en que fue generada, transmitida o recibida o en una forma en que se pueda demostrar que representa de manera

²⁰ Ibidem, pág. 234.

²¹ Ibidem, pág. 243.

²² Proyecto de Ley sobre Documentos Electrónicos de la República de Chile. Ob. cit..

precisa e inequívoca la información generada, transmitida o recibida; y si la información se mantiene de modo que sea posible identificar y autenticar el origen y el destino del documento electrónico y la fecha y hora de su transmisión o recepción (artículo 6°).

Y por último, tratándose del requisito de la escritura pública, si para cualquier efecto legal se exige la existencia o el otorgamiento de una escritura pública, o bien se prevé la existencia de consecuencias jurídicas para el evento de que falte dicha solemnidad, se entenderá que un documento electrónico cumple con esa exigencia si se ha utilizado un método o procedimiento que permita identificar a las partes comparecientes en el documento electrónico, para indicar que su contenido cuenta con la aprobación de aquellas, y que permita que las partes lo firmen en forma electrónica y un Notario o funcionario de fe, lo rubrique y le imponga un sello electrónico.

En éste Proyecto también se señala que se presumirá que la firma digital utilizada en un documento electrónico es una manifestación de voluntad del originador del documento, respecto de la intención de enviarlo, del destinatario al cual va dirigido, del contenido, y de la oportunidad y lugar de despacho del documento electrónico (artículo 24).

Por su parte, el Proyecto de Ley No. 227 de Colombia²³ prescribe que una firma digital segura será aquella que pueda ser verificada de conformidad con un sistema o procedimiento de seguridad autorizado en la Ley o por las partes, siendo un mensaje de datos firmado digitalmente aquel que se considera firmado si el símbolo o la metodología adoptada por la parte, cumple con un procedimiento de autenticación o seguridad previamente acordado, ya que cuando una firma digital ha sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de autenticar el mensaje de datos y de ser vinculado con el contenido del mismo.

Asimismo, no se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos, por lo que serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos en el Código de Procedimiento Civil, siempre que dichos mensajes cumplan con los requisitos jurídicos de observancia obligatoria establecidos en la Ley.

4.2.5. El rol del Notario.

Las principales dificultades que implica la implementación de documentos electrónicos (asegurar la integridad y la autenticidad) y de la firma digital, pueden ser fácilmente superados con la intervención de un tercero que por delegación del Estado tiene fe pública, el cual velaría por el correcto funcionamiento de la infraestructura de la firma digital e intervendría en la contratación electrónica de una forma similar a la intervención que actualmente lleva a cabo en la contratación tradicional, brindando un alto grado de certeza y seguridad jurídica. Situación posible, ya que de acuerdo al Derecho positivo vigente no existe obstáculo para que el Notario intervenga en la contratación por medios electrónicos.

²³ Proyecto de Ley No. 227 de Colombia. Ob. cit..

De conformidad con la resolución aprobada en el Primer Congreso Internacional del Notariado Latino, celebrado en Buenos Aires, Argentina “El Notario latino es el profesional del Derecho encargado de una función pública consistente en recibir, interpretar y dar forma legal a la voluntad de las partes, redactando los instrumentos adecuados a ese fin y confiriéndoles autenticidad, conservar los originales de éstos y expedir copias que den fe de su contenido. En su función está comprendida la autenticación de hechos”. Funciones previstas también en nuestro ordenamiento jurídico, en la Ley del Notariado para el Distrito Federal.²⁴ Siguiendo la misma trayectoria, en la XXIV Jornada Notarial Argentina (Buenos Aires, octubre de 1996)²⁵ se declaró que el documento electrónico es válido y eficaz como forma de contratación; que el Notariado conforme al Derecho positivo vigente está en condiciones de otorgar seguridad jurídica a la contratación por medios electrónicos en el marco de la voluntad utilizada por las partes para este fin; y que la aplicación de nuevas tecnologías en el ámbito del instrumento público requiere de la observancia de principios tales como el de intermediación, unidad de acto, actuación competente de fedatario, y demás resguardos y requisitos que hacen a la generación del instrumento de máxima jerarquía de nuestra legislación.

4.3. Sistemas de pago electrónicos.

El cumplimiento de las obligaciones y sus condiciones son previstas por nuestra legislación civil, regulando que pago o cumplimiento es la entrega de la cosa o cantidad debida, o la prestación del servicio que se hubiere prometido (artículo 2062), y que el pago deberá hacerse del modo que se hubiere pactado (artículo 2078).

Hoy en día las obligaciones cuyo objeto es dar dinero son las más frecuentes, pero los sistemas de pago, al igual que los documentos y firmas tradicionales han sido alcanzados por los crecientes desarrollos tecnológicos; surgen nuevos procedimientos de pago con las posibilidades que ofrece el medio electrónico y han sido adoptados, sobre todo por empresas debido a que sus costos resultan relativamente reducidos, mientras que garantizan seguridad, rapidez, forma práctica de uso, y confiabilidad, entre otras ventajas.

Sin embargo, los pagos realizados vía telemática no difieren mucho de aquéllos que ya se conocen (al menos por el momento); se implementan tarjetas de crédito o de débito, o “dinero virtual” que es “un esquema simple de pago por parte del cuentahabiente de un banco o institución financiera que compra o integra en una tarjeta moneda virtual con moneda real”.²⁶ Dicha tarjeta es en sí un microprocesador seguro; la duplicación, modificación involuntaria o pérdida de datos es casi imposible, ya que contiene mecanismos de autobloqueo, implementa la criptografía, y sólo el microprocesador tiene acceso a la información contenida en el mismo excluyendo la intromisión de cualquier otro sistema.

²⁴ Borja Soriano, Manuel. Ob. cit., pág. 206.

²⁵ XXIV Jornada Notarial Argentina. Ob. cit..

²⁶ Barrios Garrido, Gabriela; et al.. Ob. cit., pág. 66.

La mayor evidencia del uso cada vez más común de sistemas de pago electrónicos se da en que nuestro contacto físico con el dinero sea cada vez más esporádico, además del hecho de que los coeficientes de reserva o de liquidez de los Bancos Centrales de cada país están disminuyendo progresivamente y en proporción directa a la demanda de dinero físico;²⁷ lo que implica que probablemente en el futuro el dinero físico desaparezca y sea sustituido, por sistemas de pago basados enteramente en tecnología.

El desarrollo de medios tecnológicos cada vez mas seguros, prácticos y de uso sencillo provoca que el ideal sea, que el sistema de pago corresponda al medio digital en el que circula la información. Actualmente, la tecnología abarca casi todas las actividades humanas, pero en cuanto a los sistemas de pago electrónicos no se debe olvidar que en un principio fueron dirigidos a las grandes corporaciones que tienen mayores posibilidades de acceso a la tecnología de punta. La rápida comercialización y acceso del público en general a esta tecnología produjo que se implemente por personas que no la usan adecuadamente, de donde surge el temor del uso de estos sistemas, al ser vulnerables desde la perspectiva económica, porque tienen como base la confiabilidad de quienes los usan.

Por ello, su implementación efectiva y segura necesitará del apoyo de proyectos piloto (que algunas empresas ya están realizando) que sondeen la respuesta de la sociedad ante estos nuevos sistemas de pago.

Para analizar los nuevo sistemas de pago en un principio se debe separar a los sistemas de pago tradicionales de los de transferencia electrónica de fondos por medios telemáticos, siendo esencial dentro de estos últimos diferenciar entre si dicha transferencia se ha dado directamente entre ordenadores (debiendo existir los documentos electrónicos auténticos y seguros y que justifiquen ese pago) o si el pago se efectuó por medio de una tarjeta (dinero plástico). Pero en general, todos los nuevos sistemas de pago propuestos son instantáneos, ya que según estudios el comprador en Internet es compulsivo, además de que corresponden a la naturaleza del medio en el que circula la información.

I. Sistemas basados en tarjetas de crédito:

Los sistemas basados en tarjetas de crédito son aquéllos que necesitan en el momento de la transacción de la presentación física de la tarjeta o del número de cuenta del tarjetahabiente.

En cuanto a la seguridad de los sistemas basados en tarjetas de crédito, ésta por el momento se ha encomendado a las técnicas de encriptado, aunque Visa y Mastercard, entre otras, se encuentran desarrollando nueva tecnología.

En los sistemas basados en tarjetas de crédito el sistema SET (Secure Electronic Transaccion) ha sido el más utilizado, llegando a constituir una regla común en las transacciones electrónicas realizadas por MasterCard y Visa (desde febrero de 1998). Se caracteriza porque el número de tarjeta de crédito (encriptado o no) se transmite directamente. Este sistema permite que: se garantice la reserva en la información de

²⁷ Paladella Salord, Carlos. "El dinero físico y su desaparición?". REDI: Revista Electrónica de Derecho Informático, número 10, mayo, 1999. Disponible [Online]: <<http://derecho.org/regdi/>>

pedidos y pagos mediante la encriptación, asegurar la integridad de los datos por medio de la firma digital; la firma digital aunada a los comprobantes del comerciante permite verificar que el titular de la tarjeta de crédito sea usuario legítimo de una cuenta; garantizar la autenticidad al comerciante, al permitirle aceptar pagos con tarjetas bancarias a través de una institución financiera; y facilitar y alentar la interoperatividad entre proveedores de redes y de software.

Tanto los sistemas basados en tarjetas de crédito como aquéllos efectuados entre ordenadores (siempre que intervenga un banco) han tratado de trasladar no sólo el sistema de pago al medio electrónico sino también a los bancos mismos, así encontramos al First Bank of Internet (FBOI) como primer banco creado en Internet, en el cual algunas operaciones por razones de seguridad (por ejemplo, aperturas de cuenta) aún son realizadas por vía telefónica.

II. Sistemas de pago donde la transferencia se da directamente entre ordenadores.

Estos sistemas evitan la introducción de los datos de la tarjeta de crédito agilizando la transacción. Entre ellos se encuentran:

El FV (The First Virtual Internet Payment System o First Virtual Holdings). En este sistema de pago la operación se efectúa con la intervención de una tercera parte; se llena una forma de aplicación para que después vía telefónica se hagan del conocimiento de FV los datos de la tarjeta de crédito y se active la tarjeta; una vez activada ésta el FV enviará al usuario (por e-mail) el Virtual PIN (VPIN) que se usará para realizar cualquier transacción vía telemática.

Toda comunicación entre el usuario y el sistema de pago se hará a través de una dirección de e-mail. Así, por ejemplo, en el caso de que el usuario realice una compra da el VPIN al vendedor, quien se comunica con el FV, a su vez FV se comunica con el usuario para que confirme la compra y si lo hace FV otorga la autorización para que se efectúe el cargo en la tarjeta de crédito del usuario.

Los cheques digitales. Estos cheques se manejan de la misma forma que los cheques tradicionales, pero poseen algunas características que los identifican netamente como electrónicos: la firma digital, la encriptación, y la transmisión en línea. Así, el usuario posee una chequera electrónica, que consiste en una tarjeta (del tamaño de una tarjeta de crédito) que contiene los datos necesarios y se inserta en el slot de casi todas las computadoras portátiles; próximamente la chequera se encontrará dentro de un tarjeta inteligente (smart card).²⁸ Dentro de las empresas proveedoras de este servicio en Estados Unidos se encuentran Check Free y NetCheque.

²⁸ Dicha tarjeta cuenta con un chip que contiene un sistema operativo, aplicaciones de software, y su propia memoria, lo que le permite en el caso de los cheques digitales el llevar un registro de cheques y almacenar claves públicas y privadas.

Dinero electrónico (Electronic money, E-cash, o E-money). Para el funcionamiento del dinero electrónico intervienen instituciones de crédito las cuales envían dinero electrónico al usuario para que éste lo almacene en su ordenador, quedando a libre disposición en el momento de cualquier transacción.

Dentro de los sistemas de dinero digital se encuentran DIGICASH, NETCASH, E-CASH, CYBERCASH, y MONDEX. Entre ellos, destaca Mondex de Canadá que es una especie de tarjeta-monedero electrónico, que permite física o virtualmente realizar transacciones pagando con una reserva de valores almacenados en las tarjetas inteligentes por un banco. Aunque hasta el momento el preferido a sido Digicash al ser un sistema que brinda anonimato al pagador; vía On-line el usuario se conecta a su banco y retira una cantidad de monedas electrónicas (cospeles digitales encriptados) a cargo de su cuenta, dichas monedas digitales son almacenadas en un monedero o billetera electrónico (en este caso el disco duro del ordenador, o una tarjeta inteligente) y pueden ser utilizadas para realizar cualquier pago que desee el usuario.

Este sistema opera en el banco Mark Twain en Estados Unidos desde el 23 de octubre de 1995, pudiendo sus clientes convertir dinero real en ciberdólares y viceversa, y donde cada unidad de dinero virtual es un número que permite al banco autorizarla en relación con otras unidades, lo cual es similar al número de serie de un billete común.²⁹

Dentro de los sistemas de dinero electrónico actualmente, se distinguen dos sistemas principalmente:

1) Los que se encuentran basados en un soporte en tarjeta inteligente (card-based). La institución emisora provee a comerciantes de la tecnología necesaria para realizar la operación. En el caso del usuario, la emisión de la tarjeta se puede realizar en base a una cuenta bancaria, en máquinas expendedoras, o mediante tarjetas de crédito o de débito, y la carga de valores se realiza, por lo general, a través de un cajero automático o de un teléfono especial. Para realizar un pago se introduce la tarjeta inteligente en el slot, y se ingresa la suma a pagar, la terminal consulta el balance de la tarjeta y de ser aceptada disminuye el dinero electrónico del consumidor, y autoriza a la terminal del comerciante para que incremente su balance en la misma suma; y

2) Los que se basan en un software especial (software-based). Estos sistemas funcionan a través de un programa instalado en el ordenador del usuario; surgieron con el propósito de realizar pagos a través de las redes, por lo que su diseño depende del medio en el que se ejecute el software. En estos sistemas la carga de valores se efectúa a través de mensajes transmitidos en las redes, por lo que por razones de seguridad comúnmente se solicita la emisión de documentos comprobatorios o de cheques digitales, por las mismas razones, se opta por el uso de la firma digital para identificar al usuario con la transacción y la cantidad por la que se efectúo, permitiendo a la entidad emisora llevar un registro detallado.

En las transacciones que interviene una institución de crédito en el momento del pago, además es necesario que dicha institución posea el Common Gateway Interface (CGI) o Interfaz de Pasarela Común, y que el servidor que da alojamiento a la web pueda

²⁹ W. Kennedy y J. Dietsch citados por Hance, Olivier. Ob. cit., pág. 171.

implementarlo para permitir el entendimiento entre el banco y la página web, desgraciadamente los CGI de los bancos casi siempre difieren de los que puede implementar el servidor, ocasionando que la única solución sea cambiar de banco o de servidor, problema que se acrecienta con el hecho de que cada banco tiene un o unos CGI diferentes.

El dinero electrónico merece consideraciones especiales, dado que un futuro se prevé que sustituya al dinero físico.

El dinero es un medio de pago basado en la confianza de su aceptación por terceros que tiene las características de ser un medio de cambio, una unidad de cuenta y un depósito de valor; características que le permiten difusión y reconocimiento, y que tendrá que poseer el dinero electrónico para ser considerado dinero, siendo principalmente importante el que represente un valor por sí mismo aunque no de forma intrínseca, sin necesidad de acudir a otros respaldos. Por el momento, cada una de las formas de dinero digital (y en general de los nuevos sistemas de pago) ofrecen desventajas y ventajas, a saber:

Desventajas:

- ◆ **Confianza.** Todavía la sociedad se encuentra en un momento de transición con respecto a la transferencia de la confianza hacia los nuevos sistemas de pago, mientras que los avances tecnológicos al respecto continúan creciendo rápidamente.
- ◆ **Desconocimiento.** No se conoce por el público en general de forma detallada su funcionamiento, además de que su implementación acarrea la posibilidad de realización de operaciones nunca antes previstas ni vislumbradas gracias a las pocas limitaciones existentes.
- ◆ **El ordenamiento jurídico.** Las transacciones vía telemática necesitan de redes internacionales de conexión trascendiendo los alcances de normas nacionales e internacionales. Aún se desconoce el impacto que el dinero electrónico tendrá sobre los sistemas monetarios, y los efectos visibles de las transacciones sin fronteras no han podido ser regulados por ninguna legislación.
- ◆ **Seguridad.** Como en todos los medios tecnológicos la seguridad es de suma importancia, especialmente si se considera el surgimiento de robo de dinero electrónico, entre otros delitos informáticos. Afortunadamente, es la propia tecnología la que da las soluciones efectivas a estos problemas.
- ◆ **Falta de organización,** operación y control nacionales e internacionales adecuados para recibir al dinero digital; lo que puede provocar retraso tecnológico muy grave en los países que no adopten una estructura competitiva lo más rápido posible.

Ventajas:

- ◆ **Accesibilidad.** Se utiliza para todo tipo de transacción de forma “personalizada”.
- ◆ **Acceso global.** Se tiene acceso a todo el mundo, pues el dinero electrónico puede ser automáticamente convertido a otra moneda mediante una simple transferencia.
- ◆ **Control.** Se tiene mayor control sobre las transacciones, ya que se puede tener su seguimiento y verificación de forma eficiente (identidad de los usuarios, de los

vendedores y compradores, lugar y fecha de la transacción, entre otros) a través de los sistemas electrónicos internos de comprobación, que pueden estar contenidos desde en un ordenador hasta en una tarjeta inteligente; en todos los casos, otorgan facilidades para obtener copias de respaldo, desautorizar una transacción o controlar el pago efectivo del dinero electrónicamente.

◆ **Disponibilidad.** El dinero electrónico está disponible sin excepción a toda hora, todos los días del año; es un fenómeno globalizador que permite el contacto con cualquier parte del mundo sin necesidad de salir del lugar físico en el que nos encontremos utilizando nuestro ordenador.

◆ **Eficacia.** En algunos casos la transferencia electrónica de fondos puede realizarse incluso en segundos.

◆ **Privacidad y seguridad.** Las transacciones con dinero físico son más evidentes ante terceros, otorgando mayor privacidad y seguridad el dinero electrónico. Uno de los propósitos del dinero electrónico es el de asegurar la confidencialidad de las transacciones y el anonimato de las partes, sin embargo, este aspecto en principio positivo, se traduce en una facilidad para la infracción de normas jurídicas, como con el fraude o el lavado de dinero. Por lo que, varios países han introducido el denominado "requerimiento de reporte" que obliga a las instituciones financieras a informar a las autoridades gubernamentales sobre ciertas transacciones financieras (por ejemplo: las que exceden de diez mil dólares).

Así, se puede concluir que los nuevos medios de pago aún no han adquirido madurez y todavía existe desconfianza del público para su uso, sin embargo, la doctrina equipará esta desconfianza a la que se produjo cuando se implantó el dinero plástico, el cual hoy en día se encuentra muy arraigado.

Al no existir hasta hoy legislación creada que haya sido capaz de regular los nuevos sistemas de pago, por el momento los juristas de todo el mundo han optado por considerarlos como medios de pago apoyados en sistemas de pago preexistentes como es el caso de la tarjeta de crédito o de débito, o el dinero físico; el dinero electrónico por sí sólo aún no avala un valor. Así, en cuanto al dinero electrónico, el autor Olivier Hance opina que "Libre del mito y la subjetividad, este sistema es en realidad simple: el titular de la cuenta bancaria "compra" ciberdólares, jussando dinero real!", pero surgen importantes preguntas en cuanto a su futuro desarrollo "¿quién garantiza su estabilidad y validez? ¿No es la regulación monetaria, aun cuando sea virtual, muy importante para dejarla en manos del sector privado?"³⁰

Lo óptimo sería evitar su uso hasta crear una regulación conveniente, una estructura financiera capaz de soportar las transacciones electrónicas, y después de haber implementado proyectos piloto con éxito; por desgracia, este tipo de sistemas de pago electrónicos se utilizan todos los días y parece que nadie puede evitar su arraigamiento, convirtiéndose en un campo fértil para la legislación y el análisis jurídico.

³⁰ Hance, Olivier. Ob. cit., p.p. 166 y 174.

CAPÍTULO

V

MARCO NORMATIVO DEL DOCUMENTO ELECTRÓNICO EN MÉXICO.

El documento electrónico como soporte de la forma de contratar aún no se encuentra regulado en nuestro país, a pesar de que en muchas ocasiones es utilizado de esa manera. Sin embargo, si bien la legislación civil aún no contiene regulación expresa de determinadas consecuencias del fenómeno informático, otros ordenamientos jurídicos mexicanos ya han tratado de hacer frente a esta situación, aunque todavía no se posee en el país una estructura informática que permita una implementación integral.

5.1. Implementación del documento electrónico.

Si bien el documento electrónico como se ha expuesto a lo largo de esta investigación aún no se halla específicamente regulado en México, ya hace tiempo que documentos digitales son utilizados en nuestro país. Se usan documentos electrónicos diariamente equiparándolos a documentos escritos con una máquina de escribir, en cuyo caso son impresos y firmados de la forma tradicional, se usan como comprobantes de pago en las tiendas -tickets-, e incluso algunos ordenamientos jurídicos hacen referencia a ellos, a saber:

Código de Comercio.

El Código de Comercio establece en su artículo 48 que tratándose de las copias de cartas, telegramas y otros documentos que los comerciantes expidan, así como de los que reciban que no estén incluidos en el artículo siguiente, el archivo podrá integrarse con copias obtenidas por cualquier medio: mecánico, fotográfico o electrónico, que permita su reproducción posterior íntegra y su consulta o compulsu en caso necesario.

Código Financiero del Distrito Federal.

En Código Financiero del Distrito Federal en su artículo 84 indica que cuando las autoridades fiscales soliciten a los contribuyentes, responsables solidarios o terceros, informes, datos o documentos o pidan la presentación de la contabilidad o parte de ella, para ejercicio de sus facultades de comprobación, fuera de una visita domiciliaria, se estará a los siguiente:

I...

VII. Los informes, datos, documentos o la presentación de la contabilidad o parte de ella, requeridos por la autoridad, en visita domiciliaria o fuera de ella, deberán presentarse dentro de los siguientes plazos:

a) Los libros o registros que forman parte de la contabilidad solicitados en el curso de la visita, deberán presentarse de inmediato, así como los diagramas y el diseño del sistema de registro electrónico, en su caso...

El artículo 459 establece que las entidades que utilicen sistemas de registro electrónico de contabilidad deberán obtener de la Secretaría la autorización por escrito para la utilización de sus libros principales de contabilidad, sujetándose a las siguientes reglas:

I. Comunicarán por escrito, dentro de los treinta días siguientes a la fecha en que se adopte el registro electrónico, las características y especificaciones del sistema, señalando entre otros, marca del equipo, capacidad y características de las máquinas, lenguajes que utilicen, descripción de los programas a emplear y balanza de comprobación de saldos a la fecha en que se adopte este tipo de registro;

II. Los cambios al sistema anterior deberán comunicarse por escrito dentro de los treinta días siguientes a la fecha en que ocurran, indicando la balanza de comprobación de saldos a la fecha del cambio;

III. Las hojas sueltas de los libros diario, mayor, y de inventarios y balances se utilizarán sin que sea necesario preimprimirlas, preenumerarlas, o autorizarlas previamente, siempre que contengan el nombre y domicilio de la dependencia, órgano desconcentrado o entidad y que las máquinas respectivas impriman simultáneamente el folio consecutivo, y

IV. Los libros diario, mayor, e inventarios y balances, deberán presentarse debidamente encuadernados y foliados dentro de los noventa días posteriores a la fecha de cierre del ejercicio para su autorización respectiva.

Por su parte, el artículo 489 indica que las entidades que lleven a cabo el registro de sus operaciones financieras y presupuestales en sistemas de procesamiento electrónico de datos, deberán suministrar la información requerida por la Secretaría para la elaboración de la Cuenta Pública, en la forma y medios por ella señalados.

Ley de Comercio Exterior.

Artículo 84. Las notificaciones a que se refiere esta ley se harán a la parte interesada o a su representante en su domicilio de manera personal, a través de correo certificado con acuse de recibo o por cualquier otro medio directo, como el de mensajería especializada o electrónico...

Ley del Impuesto sobre la Renta.

En sus artículos 58 fracción X, 112 fracción VIII, y 119-I fracción VII se establece que las personas morales y las personas físicas que pertenezcan al régimen general o al simplificado de las actividades empresariales, tendrán también como obligación presentar

en el mes de febrero de cada año ante las oficinas autorizadas, declaración informativa en la que proporcionen información de las operaciones efectuadas el año anterior con los cincuenta principales proveedores, y con los clientes con los que hubieran realizado operaciones cuyo monto sea superior a \$50,000 00. Surgiendo una excepción en el caso de los contribuyentes sujetos al régimen del artículo 119-I, ya que cuando éstos realicen operaciones con el público en general no estarán obligados a presentar la información sobre clientes antes referida.

Las personas morales (artículo 58 fracción X), las personas físicas que pertenezcan al régimen general (artículo 112 fracción VIII) y las que pertenezcan al régimen simplificado de las actividades empresariales (artículo 119-I fracción VII) además de la información antes señalada deberán presentar la que se indica en el siguiente párrafo. En el caso de las personas morales no contribuyentes (artículo 72 fracción III) sólo deberán presentar la siguiente:

Información de las personas que en el mismo año les hubieren efectuado retenciones de impuesto sobre la renta, así como de los residentes en el extranjero a los que les hayan efectuado pagos de acuerdo con lo previsto en el Título V de esta ley (de los residentes en el extranjero con ingresos provenientes de fuente de riqueza ubicada en el territorio nacional), de las personas que en el año inmediato anterior les hayan efectuado pagos en los términos de los artículos 77 fracción XXX (por derechos de autor) y 141-C de esta ley (acreditamiento del impuesto para quienes cobren los ingresos por derechos de autor que se indican), y deberán proporcionar en los meses de julio de cada año y enero del siguiente, información de las personas a las que les hubieran otorgado donativos en el semestre inmediato anterior (artículos 58 fracción X, 112 fracción VIII, y 119-I fracción VII) o del que se trate (artículo 72 fracción III).

En todos los casos, cuando el contribuyente lleve su contabilidad mediante el sistema de registro electrónico, la información requerida deberá proporcionarse en dispositivos magnéticos procesados en los términos que señale la Secretaría de Hacienda y Crédito Público, mediante disposiciones de carácter general.

En el caso de los contribuyentes sujetos al régimen de los artículos 58 fracción X, 112 fracción VIII, y 119-I fracción VII además se prescribe que en los casos en que por lo menos 150 de los trabajadores del contribuyente le hayan prestado sus servicios en cada uno de los meses del ejercicio inmediato anterior, la información a que se refiere esta fracción deberá proporcionarse en los dispositivos magnéticos a que se refiere el párrafo anterior. Agregando el artículo 119-I fracción VII que lo previsto es este párrafo no será aplicable tratándose de personas físicas que se dediquen a actividades agrícolas, ganaderas, pesqueras o silvícolas. Además, tratándose de la declaración a que se refiere el artículo 83 fracción V, de esta ley (presentación de declaración anual con información de entregas a trabajadores por concepto de crédito al salario), la información sobre las retenciones efectuadas y las personas a las cuales las hicieron, deberán proporcionarse también en los términos de este artículo.

Ley Aduanera.

Artículo 38. El despacho de las mercancías deberá efectuarse mediante el empleo de un sistema electrónico con grabación simultánea en medios magnéticos en los términos que la

Secretaría establezca mediante reglas. Las operaciones grabadas en los medios magnéticos en los que aparezca la clave electrónica confidencial correspondiente al agente o apoderado aduanal y el código de validación generado por la aduana, se considera sin que se admita prueba en contrario que fueron efectuados por el agente o apoderado aduanal al que corresponda dicha clave.

El empleo de la clave electrónica confidencial que corresponda a cada uno de los agentes y apoderados aduanales equivaldrá a la firma autógrafa de éstos para todos los efectos legales.

Artículo 184. Cometan infracciones relacionadas con las obligaciones de presentar documentación y declaraciones, quienes:

I...

V. Presenten a las autoridades aduaneras la información estadística de los pedimentos que formulen, grabada en un medio magnético, con información inexacta, incompleta o falsa.

VI. Transmitan en el sistema electrónico o consignen en el código de barras impreso en el pedimento o en cualquier otro medio de control que autorice la Secretaría, información distinta a la declarada en dicho documento. La falta de algún dato en la impresión del código de barras no se considerará como información distinta, siempre que la información transmitida al sistema de cómputo de la aduana sea igual a la consignada en el pedimento...

Código Fiscal de la Federación.

Artículo 45. Los visitados, sus representantes o la persona con la que se entienda la visita en el domicilio fiscal, están obligados a permitir a los visitadores designados por las autoridades fiscales...la verificación de bienes y mercancías, así como de los documentos, discos, cintas o cualquier otro medio procesable de almacenamiento de datos que tenga el contribuyente en los lugares visitados.

Cuando los visitados lleven su contabilidad o parte de ella con el sistema de registro electrónico, o microfilm o graben en discos ópticos o en cualquier otro medio que autorice la Secretaría de Hacienda y Crédito Público, mediante reglas de carácter general, deberán poner a disposición de los visitadores el equipo de cómputo y sus operadores, para que los auxilien en el desarrollo de la visita.

Cuando se dé alguno de los supuestos que a continuación se enumeran, los visitadores podrán obtener copias de la contabilidad y demás papeles relacionados con el cumplimiento de las disposiciones fiscales, para que, previo cotejo con los originales, se certifique por los visitadores:

I...

IX. Si el visitado, su representante o la persona con quien se entienda la visita se niega a permitir a los visitadores el acceso a los lugares donde se realiza la visita; así como a mantener a su disposición la contabilidad, correspondencia o contenido de cajas de valores.

En los supuestos a que se refieren las fracciones anteriores, se entenderá que la contabilidad incluye, entre otros, papeles, discos y cintas, así como cualquier otro medio procesable de almacenamiento de datos...

Artículo 53. En el caso de que con motivo de sus facultades de comprobación, las autoridades fiscales soliciten datos, informes o documentos del contribuyente, responsable solidario o tercero, se estará a lo siguiente:

I. Se tendrán los siguientes plazos para su presentación:

a) Los libros y registros que formen parte de su contabilidad, solicitados en el curso de una visita, deberán presentarse de inmediato, así como los diagramas y el diseño del sistema de registro electrónico en su caso...

Ley Federal del Derecho de Autor.

Artículo 27. En él se establece que los titulares de los derechos patrimoniales podrán autorizar o prohibir la reproducción, publicación, edición o fijación material de sus obras en copias o ejemplares, efectuada por cualquier medio incluyendo el electrónico; asimismo, la comunicación pública de su obra podrá darse a través de la telecomunicación.

Por su parte, el artículo 123 prescribe que el libro es toda publicación unitaria, no periódica, de carácter literario, artístico, científico, técnico, educativo, informativo o recreativo, impresa en cualquier soporte, cuya edición se haga en su totalidad o de una sola vez en un volumen o a intervalos en varios volúmenes o fascículos. Comprenderá también los materiales complementarios en cualquier tipo de soporte, incluido el electrónico, que conformen, conjuntamente con el libro, un todo unitario que no pueda comercializarse separadamente.

Antigua Ley del Seguro Social.

En el artículo 19 último párrafo, se hace referencia a la posibilidad de que el patrón lleve la contabilidad mediante el sistema de registro electrónico. Y se le permite que presente información como altas y bajas de los trabajadores, las modificaciones de sus salarios (y las que señale esta ley y sus Reglamentos), y registros (nóminas o listas de raya) en los que se asiente el número de días trabajados y los salarios percibidos por los trabajadores (y demás que señale esta ley y sus reglamentos), entre otros, en dispositivos magnéticos procesados en los términos que señale el Instituto.

De los ordenamientos jurídicos antes señalados se desprende que el documento electrónico es un soporte diferente al papel, que no afecta la naturaleza jurídica del acto mismo; que las claves electrónicas confidenciales son equiparables a la firma autógrafa y con ellas se cumple el requisito de autenticación; que los requisitos y medidas de seguridad que deben contener los documentos digitales deben ser establecidos por una autoridad, en la mayoría de estos casos por una Secretaría; que los medios telemáticos son efectivos para la transmisión de documentos; y que los equipos usados tendrán que ser compatibles con los utilizados por la autoridad, o en caso de que se requiera la información en ellos

contenida se deberán proporcionar también los medios necesarios para hacerla humanamente entendible; pero es la Ley del Mercado de Valores la que ahonda en el tema del documento informático:

Ley del Mercado de Valores.

El documento electrónico está siendo implementado en la contratación bursátil en México, en su artículo 90 regula a la contratación bursátil estableciendo que "Las operaciones que las casas de bolsa celebren con su clientela inversionista y por cuenta de la misma, se registrarán por las previsiones contenidas en los contratos de intermediación bursátil, que al efecto celebren por escrito, salvo que, como consecuencia de lo dispuesto en ésta u otras leyes, se establezca una forma de contratación distinta.

Por medio del contrato de intermediación bursátil, el cliente conferirá un mandato general para que, por su cuenta, la casa de bolsa realice las operaciones autorizadas por esta ley, a nombre de la misma casa de bolsa, salvo que, por la propia naturaleza de la operación, deba convenirse a nombre y representación del cliente, sin que en ambos casos sea necesario que el poder correspondiente se otorgue escritura pública".

Ese ordenamiento en su artículo 91 señala que como consecuencia del contrato de intermediación bursátil:

I..

II. A menos que en el contrato se pacte el manejo discrecional de la cuenta, las instrucciones del cliente para la ejecución de operaciones concretas o movimientos en la cuenta del mismo, podrán hacerse de manera escrita, verbal o telefónica, debiéndose precisar en todo caso el tipo de operación o movimiento, así como el género, especie, clase, emisor, cantidad, precio y cualquiera otra característica necesaria para identificar los valores materia de cada operación o movimiento en la cuenta.

Las partes podrán convenir libremente el uso de carta, telégrafo, telex, telefax o cualquier otro medio electrónico, de cómputo o telecomunicaciones para el envío, intercambio o, en su caso, confirmación de las órdenes de la clientela inversionista y demás avisos que deban darse conforme a lo estipulado en el contrato, así como los casos en que cualquiera de ellas requiera cualquier otra confirmación por esas vías...

V. En caso de que las partes convengan el uso de medios electrónicos, de cómputo o de telecomunicaciones para el envío, intercambio y, en su caso, confirmación de las órdenes y demás avisos que deban darse, habrán de precisar las claves de identificación recíprocas y responsabilidades que conlleve su utilización.

Las claves de identificación que se convenga utilizar conforme a este artículo sustituirán a la firma autógrafa por lo que las constancias documentales o técnicas en donde aparezcan, producirán los mismos efectos que las leyes otorguen a los documentos suscritos por las partes y, en consecuencia, tendrán igual valor probatorio...

Por su parte, el artículo 100 prescribe que la falta de forma escrita exigida por esta ley o por convenio de las partes, respecto de los actos o de las operaciones que sean contratadas entre las casas de bolsa y su clientela inversionista, produce la nulidad relativa de dichos actos u operaciones...

Cuando las partes hayan convenido el uso del telégrafo, telex, telefax, o cualquier otro medio electrónico, de cómputo o de telecomunicaciones conforme al segundo párrafo de la fracción II del artículo 91 de la presente ley, las modificaciones a los contratos que tengan celebrados podrán realizarse a través de los mismos, observando el plazo y las modalidades para la manifestación del consentimiento a que se refiere este artículo.

En cuanto a la automatización son los artículos 112 a 117 los que hacen referencia a este aspecto de la siguiente manera:

Artículo 112. Las casas de bolsa, especialistas bursátiles, bolsa de valores, instituciones para el depósito de valores e instituciones calificadoras de valores, sin perjuicio de lo señalado en el Código de Comercio, en la presente ley y en las demás disposiciones conducentes, deberán llevar su contabilidad y el registro de las operaciones en que intervengan, mediante sistemas automatizados, o por cualquier otro medio, conforme a lo que señale la Comisión Nacional de Valores.

Artículo 113. Los sistemas automatizados a que se refiere el artículo anterior, deberán reunir las características que, mediante disposiciones de carácter general, determine la Comisión Nacional de Valores, considerando criterios de seguridad en su funcionamiento y verificación accesible de la información, observándose en todo caso lo siguiente:

I. La compatibilidad técnica con los equipos y programas de la Comisión Nacional de Valores;

II. Los asientos contables y registros de operación que emanen de dichos sistemas, expresados en lenguaje natural o informático, se emitirán de conformidad con las disposiciones legales en materia probatoria, a fin de garantizar la autenticidad e inalterabilidad de la información respecto a la seguridad del sistema empleado; y

III. El uso de claves de identificación en los términos y con los efectos señalados en el artículo 91, fracción V de esta ley.

Artículo 114. La información que en términos de esta ley y de las disposiciones de carácter general que de ella deriven, deben proporcionar a la Comisión Nacional de Valores las entidades a que se refiere el artículo 112, provenientes de sistemas automatizados, se pondrán a disposición de dicha autoridad por cualquiera de estas formas:

I. Envío a través de medios telemáticos, es decir, originada en equipos informáticos y de telecomunicación.

II. Entrega en soportes materiales de información acordes a la compatibilidad técnica expresada en la fracción I del artículo 113.

La información, una vez recibida por la Comisión Nacional de Valores a través de cualquiera de estas formas, ya no podrá ser modificada o sustituida por la entidad emisora o la autoridad receptora, salvo por determinación expresa de la Comisión o, en su caso, de otras autoridades competentes, con motivo de las correcciones que sean estrictamente necesarias, o bien del esclarecimiento de hechos y eventual deslinde de responsabilidades.

Las emisoras de valores inscritas en el Registro Nacional de Valores e Intermediarios, para el envío o entrega a la Comisión Nacional de Valores, a la bolsa de valores correspondiente y al público de carácter general que de ella deriven, deberán utilizar los

medios a que se refiere este artículo, con arreglo a las disposiciones de carácter general que al efecto expida la misma Comisión.

Lo anterior, sin perjuicio de que la Comisión Nacional de Valores requiera en cualquier tiempo la información de que se trate, la cual deberá serle proporcionada por escrito y con la firma autógrafa de quienes deban suscribirla.

Artículo 115. La Comisión Nacional de Valores debe estar provista de los sistemas automatizados para la recepción, resguardo y clasificación de la información que le sea proporcionada de acuerdo con el artículo anterior, así como la que recabe de equipos telemáticos o en soportes materiales de información en ejercicio de las facultades de inspección y vigilancia que tiene atribuidas.

A la citada Comisión le será aplicable, en lo conducente, lo dispuesto en el artículo 113 del presente ordenamiento.

Artículo 116. La información contenida en soportes materiales, o bien proveniente de procesos telemáticos, siempre que esté validada por la autoridad receptora y la entidad emisora, de acuerdo a las características y dentro de los plazos que determine mediante disposiciones de carácter general la Comisión Nacional de Valores, así como la información que cumpliendo con dicho procedimiento se integre a las bases de datos de la propia Comisión, producirán los efectos que las leyes otorgan a los documentos originales y, en consecuencia, tendrán igual valor probatorio, y

Artículo 117. Las disposiciones de este Capítulo serán aplicables a las sociedades de inversión y a las sociedades operadoras de sociedades de inversión, en las materias correspondientes.

5.1.1. Ventajas económicas y sociales.

La correcta implementación de los soportes informáticos y medios telemáticos, trae como principal ventaja el desarrollo de la tecnología, y en consecuencia del Internet. Internet provee de diversos servicios, productos e ideas; es hasta hoy el sistema internacional más grande de intercambio de información en forma casi instantánea, permitiendo el desarrollo de la ciencia, el arte, la cultura y de las relaciones interpersonales.

Al ser Internet un medio que pugna por la eliminación de barreras tiempo-espaciales, sociales e idiomáticas, entre otras, en muchas ocasiones con el único objetivo de lograr el bien común, incluso se ha llegado a considerar que con un avance adecuado su servicio será primordialmente ventajoso para personas de tercera edad, discapacitados, ciudadanos que viven en zonas rurales y para la pequeña empresa, al facilitar acceso a la información, a la educación y a la promoción tanto de empresas como de organizaciones de caridad.

Pero, debe tenerse en cuenta que en nuestro país aún se necesita de un cambio cultural para la aceptación de estas nuevas tecnologías que se han manifestado como el mejor medio de satisfacción de muchas necesidades, debiéndose ante todo tener una identidad nacional consolidada, porque este cambio implica un encuentro cultural e ideológico continuo con el resto del mundo. Este cambio se dará probablemente como natural adaptación a lo que el medio nos impone.

La "Revolución Digital" exige interdisciplinariedad adjunta de preparación de profesionales calificados y numerosos replanteamientos conceptuales de la realidad misma, lo que es un cambio necesario, al ser la propia sociedad la que busca la forma de satisfacer sus necesidades y si en este momento la mejor forma es la tecnológica se debe respetar a la nueva era, no permitiendo que el temor gobierne nuestra forma de actuar, sin que ello implique actos impulsivos o el olvido de las debidas medidas de precaución.

En el aspecto económico según un estudio realizado por la firma Killen & Associates de California,¹ se considera que en los próximos diez años todas las transacciones efectuadas por catálogo, televisión, transferencia electrónica de datos (EDI: Electronic Data Interchange), y redes On-line se trasladarán a Internet. Asimismo, se prevé que en el año 2000 se realizarán compras de bienes y servicios en la Red por US\$600 billones, y por US\$ 1,5 trillones en el 2005; calculando un cargo (*fee*) de US\$1,50 por transacción, las organizaciones que utilicen el Internet para realizar sus operaciones obtendrán ganancias de US\$ 11 billones en el 2000 y US\$ 26 billones en el 2005, contra un costo aproximado del 50 al 60% de dichas cantidades.

Este es un año en que el comercio electrónico se ha desarrollado de forma impresionante al ser un mercado global con costos relativamente reducidos, lo cual no ha sido sorprendente, desde 1997 el Vicepresidente de los Estados Unidos, Al Gore, manifestó que Internet puede crear un mercado mundial para cualquier cosa, permitiendo a los consumidores una comparación de precios nunca antes vista y un mercado virtual accesible todos los días a toda hora.²

Los medios telemáticos aumentan la capacidad de oferta y de demanda, la posibilidad de elección entre productos y servicios de todo el mundo con la correspondiente comparación de precios, permiten que se elimine en lo posible a los intermediarios y que se ahorre tiempo y capital al público en general y a los empresarios, quienes en vez de tener que recurrir a diversas vías, por ejemplo a la vía telefónica y al correo, pueden realizar varias operaciones usando una vía única, la telemática.

Así, en cuanto a las redes, si bien las redes cerradas posibilitan un mayor grado de seguridad -ya que se conoce a propietarios y administradores y no se admite el ingreso de terceros no autorizados-, los avances más importantes se han dado en las redes abiertas, al ser éstas las que revisten cada vez mayor importancia para la comunicación global, las que ofrecen nuevas posibilidades empresariales, las que permiten la reducción de costos, las que brindan herramientas que mejoran la productividad, así como las que ofrecen un mercado mundial abierto las 24 horas del día todos los días del año, y las que prometen convertirse en el eje de la economía mundial.

Asimismo, la información es un bien inmaterial con un soporte material que le da disponibilidad, es "un bien susceptible de apropiación con un innegable valor patrimonial

¹ Devoto, Mauricio; Lynch, Horacio M. Op. cit.

² Gore, Al. Transcripción de las palabras que el Vicepresidente de los Estados Unidos dirigió el 1º de julio de 1997 en ocasión del informe a la Casa Blanca sobre la Estructura del Comercio Electrónico. Cuestiones Mundiales, Publicación Electrónica del Usis, volumen 2, octubre, 1997. Disponible [Online]:<<http://www.usia.gov/journals/itgic.htm>>

inherente”.³ Representa un bien con fuerza económica tan importante que ha sido reconocida por la UNESCO, la información es esencial para la toma de decisiones, es un bien de alto costo con gran rentabilidad, por lo que se le ha llegado a comparar con las materias primas.

La información es poder, un trato incorrecto de la misma implicaría el acrecentamiento de la brecha entre ricos y pobres, entre los que poseen información y los que carecen de acceso a la misma, de donde emana la importancia de el establecimiento de una infraestructura nacional de la información planeada dentro y acorde con la política nacional, benéfica a toda la sociedad mexicana.

La “Revolución Digital” es un fenómeno insoslayable y constituye nuestra realidad, por lo que no debemos temerle ni rehuirle, sino adaptarnos a ella de la mejor manera posible e incluso obtener provecho de esta Revolución. Implica un progreso al que debemos sumarnos, el país que se retrase en hacerlo perderá de forma importante su competitividad lo que trae aparejadas implicaciones económicas y por ende sociales (calidad de vida, salarios, etcétera) desastrosas.

5.1.2. Aspectos positivos de la regulación jurídica del documento electrónico.

La regulación relativa a aspectos informáticos no es sencilla, debe comenzar por un estudio interdisciplinario de todas las tecnologías, para escoger las susceptibles de garantizar que el documento electrónico cumpla con los requisitos jurídicos necesarios para ser equiparable al documento tradicional, sin embargo, no se aconseja establecer detallada y específicamente la selección de determinadas tecnologías en las leyes, dado que el desarrollo tecnológico se da a cada momento lo cual podría provocar que algunas de estas elecciones fueran obsoletas en poco tiempo; de la misma manera en cuanto a la selección lexicológica a utilizar ésta deberá ser apropiada para dar un significado homogéneo a los términos empleados, tratando de evitar leyes demasiado técnicas por la razón antes mencionada, además de que las leyes deben ser escritas para el conocimiento de la población en general.

Asimismo, en cuanto a la legislación del documento electrónico se debe tener en cuenta su carácter mundial y que la eficacia de estas leyes dependerá en mucho de su uniformidad a nivel estatal e internacional, la que en ocasiones tendrá que ser reforzada con tratados internacionales; ya que como se ha visto (por ejemplo, con el Internet) su aplicación es a un entorno global, en donde diferencias radicales entre las legislaciones obstaculizarían el desarrollo de las relaciones interpaíses y de la tecnología misma.

Por lo que, la tarea del Congreso Federal no es fácil, en principio, fue recientemente cuando el fenómeno informático despertó el interés de nuestros legisladores los cuales carecen de la debida preparación técnica al respecto, además de que se debe cuidar de la

³ Téllez Valdes, Julio. Ob. cit., pág. 65.

técnica jurídica, conjugar aspectos técnico-jurídicos, y legislar sobre un fenómeno que ha progresado sin los debidos límites legales, lo que ha permitido la creación de intereses empresariales millonarios; sin embargo, no puede regularse apresuradamente ni sin tomar todas las consideraciones necesarias, y siempre se debe tener en cuenta como un punto a favor, la experiencia legislativa recabada por otros países adaptándola a nuestra realidad nacional.

Hasta el momento, gran parte del desarrollo tecnológico y sus implicaciones se han otorgado al sector privado, y diversas cuestiones relacionadas con soportes informáticos y medios telemáticos se han dejado a la costumbre y la buena fe, desgraciadamente en el entorno que vivimos actualmente lo anterior se traduce en la existencia de incertidumbre en cuanto a la aplicación del Derecho, y en la necesidad de que el sector público cree una infraestructura mexicana de la información. Gran parte de los países de primer mundo ya poseen esa infraestructura, como Estados Unidos con la denominada Infraestructura Nacional de Información (NII: National Information Infrastructure); ello implica que México posee un rezago tanto estructural como legislativo al respecto, lo cual debe corregirse para asegurar la competitividad de nuestro país, y la implementación correcta de la informática que necesariamente va unida a nuestra realidad social y económica.

Una correcta regulación permitirá el desarrollo tecnológico y de las nuevas formas de relación humana; la satisfacción eficiente de necesidades sociales; y la existencia de un medio donde la información se transmita de manera rápida y eficaz y que incluso provea de medios probatorios como son los documentos electrónicos, brindando la seguridad jurídica y técnica requerida.

En el caso específico de México, se considera necesario que la Comisión de Informática, funcione como organismo en el que confluyan libre y decididamente, la totalidad de los actores involucrados en el universo de la información, cuya titularidad forzosamente deberá recaer en aquel legislador que tenga los conocimientos legales y telemáticos suficientes para establecer de forma consensada, intersectorial y supranacionalmente los criterios normativos que en la próxima centuria deberán aplicarse a las comunicaciones en línea y a las actividades que mediante éstas se desarrollen.⁴

En nuestro país, se opina que la exigencia jurídico procesal de la firma ológrafa es el principal obstáculo para la implementación del documento electrónico, al menos mientras no se prevea en las disposiciones legales aplicables al efecto.

5.2. Reconocimiento legal del documento electrónico como forma de contratación.

La "Revolución Digital" se inició como una conducta social, siendo nuestra realidad la de vivir en una aldea global, donde la evolución tecnológica avanza continuamente sin

⁴ Hernández, Luis Antonio. "Internet y Legislación. Comercio electrónico, una tarea incompleta". El Universal, Universo de la Computación, lunes 17 de mayo de 1999, pág. 9.

esperar a ser jurídicamente regulada, dejando a abogados y legisladores rezagados y en gran desventaja si se toma en cuenta que tienen que abarcar de manera legal un fenómeno que hace tiempo que se desarrolla y que supera en gran medida cualquier previsión o expectativa del futuro que se haya tenido.

Para lograr un adecuado reconocimiento de valor jurídico del documento electrónico no bastará la jurisprudencia, como ya numerosos países lo han demostrado, se deberá crear una normativa específica la cual es aún más necesaria si se toma en consideración que los documentos con soporte informático han afectado radicalmente conceptos tradicionalmente arraigados, como el de soporte en papel y el de la autenticidad.

La legislación referente al documento electrónico requiere de ciertas consideraciones fundamentales en cuanto a los aspectos no regulados, entre ellas se encuentran el que en caso de existir criterios jurisprudenciales como reflejo de la realidad práctica, estos deben ser tomados en consideración; debe analizar las normas preexistentes a fin de evaluar su posible aplicación análoga o la expansión de ciertos conceptos; y la creación de un nuevo ordenamiento jurídico (integrado a los ordenamientos existentes o la creación de una ley específica). Asimismo, algunas normas se deberán derogar, otras ser modificadas, y algunas más ser creadas, y no sólo se deberá establecer la validez jurídica del documento electrónico, sino se deberán hacer todas las consideraciones al respecto detallando la infraestructura técnica y operacional para la inserción del mismo dentro del orden jurídico.

5.2.1. Análisis de los artículos 1832, 1833 y 1834 del Código Civil para el Distrito Federal y propuesta de reforma.

El artículo 1832 regula que “En los contratos civiles cada uno se obliga en la manera y términos que aparezca que quiso obligarse, sin que para la validez del contrato se requieran formalidades determinadas, fuera de los casos expresamente designados por la ley”; establece el principio de libertad de formas, en virtud del cual las partes pueden adoptar libremente el soporte informático como soporte de la forma de exteriorización del consentimiento, limitados sólo por las excepciones establecidas en la ley; por lo que este artículo no requerirá reforma alguna para la aceptación del documento electrónico.

Por su parte, en el artículo 1833 se incluye la acción para que se dé al contrato la forma legal indicando que “Cuando la ley exija determinada forma para un contrato, mientras que éste no revista esa forma no será válido, salvo disposición en contrario; pero si la voluntad de las partes para celebrarlo consta de manera fehaciente, cualquiera de ellas puede exigir que se dé al contrato la forma legal”, este artículo tampoco requiere de reforma; pero en el caso del artículo 1834 que prescribe que “Cuando se exija la forma escrita para el contrato, los documentos relativos deben estar firmados por todas las personas a las cuales se les imponga esa obligación. Si alguna de ellas no puede o no sabe firmar, lo hará otra a su ruego y en el documento se imprimirá la huella digital del interesado que no firmó”, se propone que éste se reforme para incluir que cuando se exija la forma escrita para el contrato, los documentos relativos incluyendo los electrónicos, deben estar firmados por todas las personas a las cuales se les imponga esa obligación...Tratándose de documentos

electrónicos, se cumple con el requisito de escrituración, si la información contenida en el mismo es legible, está íntegra y se halla disponible de ser presentada en cualquier momento; y con el requisito de firma, si se ha utilizado un método confiable que permita lograr la autenticación, en cuyo caso las claves de identificación sustituirán a la firma autógrafa.

CONCLUSIONES

- 1.- El desarrollo de la informática y principalmente del Internet, ha producido un fenómeno global que ha transformado al mundo en cuanto a los medios a través de los cuales las personas se relacionan, siendo el Derecho Informático aquél que se encarga del estudio de los efectos jurídicos que dicho fenómeno pueda acarrear.
- 2.- El documento electrónico en sentido amplio, no ha implicado cambios fundamentales en nuestra forma de concebir a los documentos al ser directamente comprensibles por el hombre; sin embargo el documento digital en sentido estricto, al implicar un nuevo soporte para la información, trae aparejadas importantes diferencias con el documento tradicional con soporte papel a saber: el soporte del documento electrónico es un medio magnético u óptico, ocasionando que no pueda ser directamente conocido por el hombre, necesitándose para ello de máquinas traductoras especializadas; su medio de representación es el informático a través de una computadora; no se le puede aplicar la firma manuscrita; contiene mayor cantidad de información; y permite una recuperación y transmisión de datos más rápida y efectiva.
- 3.- El documento electrónico en sentido estricto reúne los elementos necesarios para ser equiparado al documento escrito, al ser una representación de hechos y/o actos jurídicos grabados sobre una superficie o soporte informático, lo que permite su posterior consulta y conservación a través del tiempo.
- 4.- Al no poderse aplicar la firma manuscrita al documento digital, se le aplica la firma electrónica; la cual consiste en su medio más usado, en claves únicas asignadas a las partes de una relación jurídica, permitiendo asegurar la integridad y autenticidad de los documentos.
- 5.- La firma electrónica más utilizada hasta ahora emana de la criptografía, la cual consiste en matemáticas aplicadas para convertir textos legibles en textos ilegibles y viceversa.
- 6.- La contratación electrónica no afecta el contenido intrínseco de los actos, sino que simplemente cambia los medios de exteriorización de la voluntad de las partes; así el contrato electrónico es el convenio por el cual se crean o transfieren derechos y obligaciones usando medios informáticos para ello.
- 7.- El uso y eficacia de los medios telemáticos, en general, y de Internet, en específico, se ha extendido hasta la materia civil con implicaciones jurídicas en el aspecto contractual; entre ellas el de una nueva forma de contratar, por lo que debe reconocerse al documento electrónico como válido y eficaz como forma de contratación entre presentes o ausentes, y aceptarse el uso de la firma digital.

8.- Ya no se encuentra en discusión si la informática y la teleinformática deben o no ser reguladas, sino como incluirlas en el ordenamiento jurídico; su marco normativo debe permitir su desarrollo, ser compatible con los derechos establecidos en nuestra Carta Magna y en nuestras leyes, evitar su empleo indebido, promover la cooperación internacional, garantizar la seguridad, ser uniforme, y utilizar el Derecho comparado.

9.- En una sociedad que cada día es más dependiente de la tecnología de la información, el estudio de los medios informáticos implica un desafío que debe ser aceptado por los abogados. Este estudio debe tener en cuenta múltiples factores, como son el social, el técnico, y el jurídico, donde el abogado basado en los conceptos tradicionales del Derecho deberá darles nueva perspectiva para adecuar la realidad jurídica a la realidad social imperante.

GLOSARIO

TÉRMINOS BÁSICOS SOBRE LA ESTRUCTURA Y EL FUNCIONAMIENTO DE LAS COMPUTADORAS.

Computadora, ordenador. Es un dispositivo electrónico capaz de recibir, procesar, almacenar y proporcionar información a gran velocidad. Entre ellas han adquirido importancia las PC's (Computadora Personal) que satisfacen las necesidades de una persona.

Las computadoras se clasifican por:

* Su diseño (forma en que representan sus datos) en **analógicas** que son aquellas que representan sus datos en base a la cantidad de voltaje; y en **digitales**, que son las que representan sus datos por el paso de la corriente eléctrica.

* Su tamaño (dimensiones del equipo) en:

Mainframes o macro-computadoras.- Son de gran dimensión, manejan grandes cantidades de información y normalmente se utilizan para la operatividad de redes.

Minicomputadoras.- Son de menor tamaño que las anteriores pero con gran capacidad.

Microcomputadoras o computadoras personales (PC's).- Fueron diseñadas para satisfacer las necesidades de una persona funcionando adecuadamente.

Dos partes esenciales conforman a la computadora, el hardware y el software, en el caso de que alguna de ellas faltará la computadora no sería útil.

Estructura de las computadoras:

Hardware. El hardware se encuentra conformado por toda parte de la computadora que es visible y físicamente palpable.

Periférico. Conforman parte del hardware, y es una pieza del mismo unido a la computadora, es todo dispositivo asociado a una computadora que permite la comunicación entre ésta y el usuario.

Tradicionalmente se clasifican en periféricos de entrada, salida y de entrada/salida.

- **Periféricos de entrada.** Son aquéllos que permiten al usuario proporcionar información e instrucciones a la computadora. Ejemplos: Teclado, mouse o ratón, escáner, vídeo, joystick.
- **Periféricos de salida.** Permiten a la computadora hacer del conocimiento del usuario determinada información, por medio de letras o gráficos a través del monitor o de la

impresora, o por sonidos a través de las bocinas, entre otros. Ejemplo: Monitor, impresora, bocinas.

- **Periféricos de entrada/salida, de almacenamiento o memoria auxiliar.** Estos periféricos leen y registran información en soportes idóneos para ello. Ejemplos: Disco duro, disquetes, CD-ROM, cartuchos, CD-WORM, cinta.

Software. El software no es visible ni palpable, por lo que lo se encuentra constituido por todo lo inmaterial o lógico del ordenador, es decir, por aquellas instrucciones electrónicas que guían internamente el funcionamiento del ordenador.

Dentro del software se pueden reconocer los lenguajes y la paquetería o programas de aplicación.

- **Lenguajes.** Serie de comandos organizados lógicamente de tal manera que permitan una comunicación entre el usuario y el ordenador indicándole a este último la forma en que ha de trabajar. Dentro de ellos se encuentran los sistemas operativos, los cuales se crean con el fin de controlar todas las actividades de la computadora.
- **Programas de aplicación.** Conjunto de comandos que al ejecutarse por un ordenador acarrear como consecuencia la realización de tareas específicas.

Funcionamiento de las computadoras.

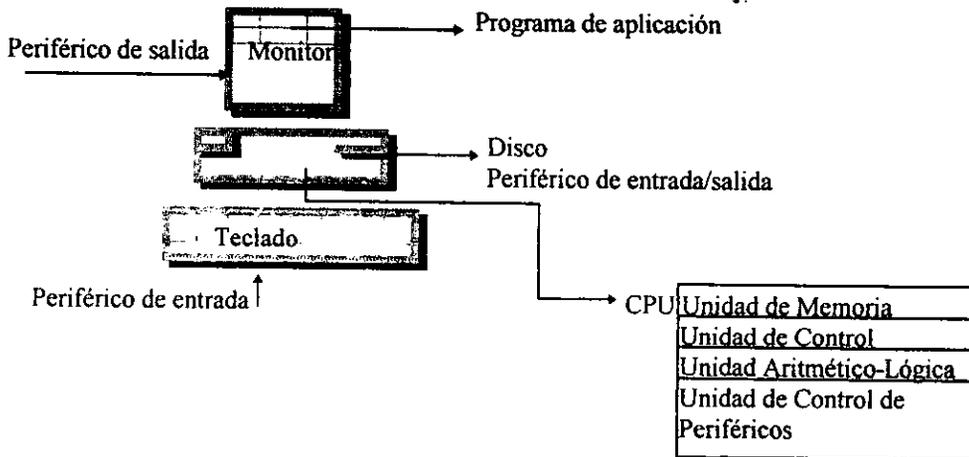
Unidad Central de Procesamiento (CPU) o procesador. Está Unidad se encarga de controlar y supervisar el sistema de cómputo como una unidad, de procesar instrucciones, realizar operaciones matemáticas y lógicas, y controlar el envío y recepción de datos desde y hacia los periféricos, por lo que se le considera como el cerebro de la computadora.

Se encuentra conformado por:

- **La Unidad de Memoria.** Es un depósito para la información que se ha de procesar, a su vez se integra por la unidad de almacenamiento, la unidad de control de memoria y el registro de dirección de datos.
- **La Unidad de Control.** Se encarga de interpretar y ejecutar los comandos, así como de controlar la operación de todas las partes integrantes del sistema de cómputo.
- **La Unidad Aritmético-Lógica.** Ejecuta las operaciones matemáticas (suma, resta, multiplicación y división) y lógicas (No, Y, O) básicas con las que toda la información es procesada.
- **La Unidad de Control de Periféricos.** Controla el tráfico de datos proveniente de los periféricos, y se encarga de determinar si es posible o no enviar dicha información a esos periféricos para que efectúen su función.

Memoria RAM (Memoria de acceso aleatorio). Almacena de forma temporal información, por lo que al apagar la computadora la información en ella almacenada se perderá. La información en ella almacenada puede ser modificada tantas veces sea necesario.

Memoria ROM (Memoria de solo lectura). Contiene información que una vez almacenada es inalterable, por lo que en ella se almacena el software que el fabricante considera como indispensable para el funcionamiento esencial de la computadora.



TÉRMINOS BÁSICOS SOBRE LA ESTRUCTURA Y EL FUNCIONAMIENTO DE INTERNET.

Internet. Es la red de redes, al ser la red abierta de computadoras más grande del mundo, es una red de uso general que permite el intercambio internacional de información. Es un conjunto de redes que se comunican entre sí utilizando el Protocolo de la Internet. Dentro de los servicios de Internet se encuentran:

- **El correo electrónico (e-mail).** Funciona de forma similar al servicio postal, por lo que se usa para el envío y recepción de mensajes. Para utilizarlo, al igual que con el correo común es necesario poseer una dirección, sólo que en este caso debido al medio en el que transita la información la dirección será una de correo electrónico.
- **Conversaciones en línea (IRC: Internet Relay Chat).** Es un servicio usado para "charlar" en tiempo real con otros usuarios cuyas computadoras se encuentren interconectadas en el momento de la sesión.
- **Boletines electrónicos (BBS: Bulletin Board Systems).** Se usan para difundir información específica.
- **Telnet.** Permite a través de la interconexión y de forma interactiva el acceso remoto a sistemas, programas o aplicaciones disponibles en otro ordenador.
- **Protocolo de Transferencia de Archivos (FTP: File Transfer Protocol).** Constituye una versión reducida de Telnet al únicamente usarse para transferir archivos.
- **Grupos de discusión o foros.** Los foros no implican al correo electrónico y en ellos se intercambia información sobre un tema en particular. Sin embargo, la comunicación no se da en tiempo real ni directamente entre los participantes, ya que cada uno deja su punto de vista o aportación para que posteriormente otro miembro del grupo lo consulte.
- **World Wide Web (WWW o Web).** Permite hacer una consulta y transmitir información gracias a los enlaces de hipertexto insertados por el autor de dicha página.

Funcionamiento. Funciona a través de:

Anfitriones. Computadoras directamente conectadas a alguna de las redes que forman Internet.

Hipertexto. Texto realzado, por lo general con subrayado.

HTTP (Protocolo de Transferencia de Hipertexto). Serie de enlaces que permiten que dentro del ambiente de Internet se pueda saltar de una página a otra usando el hipertexto.

Módem. Dispositivo que permite al ordenador comunicarse con otros equipos a través de vías telefónicas.

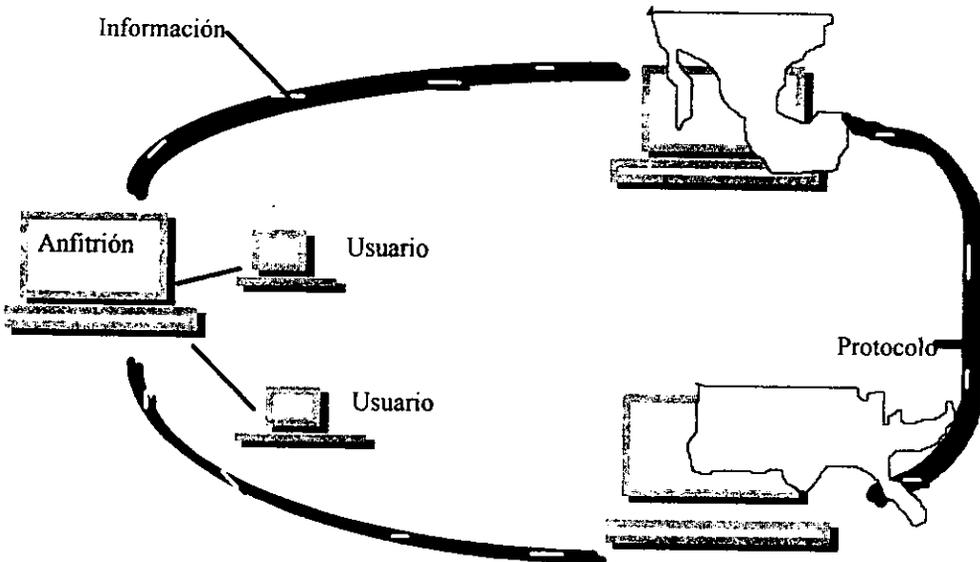
Navegador o browser. Programa que permite visualizar y facilita la búsqueda y obtención de información en la Web.

Protocolo. Regla comúnmente aceptada para transmitir y recibir información.

Protocolo de la Internet (IP). Lenguaje que las computadoras utilizan para comunicarse entre ellas en el ambiente Internet y que se encuentra diseñado para soportar miles de redes de trabajo.

Sistema de Nombre de Dominio. Nombres asignados a las computadoras, éstos consisten en series de letras seccionadas por puntos, donde las secciones corresponden a la zona (categoría general dentro la que se puede encuadrar al uso que el usuario le da a la computadora), al nombre de la compañía, y al nombre del ordenador.

Usuario. En Internet se les denomina así a las computadoras conectadas a alguno de los anfitriones para lo cual necesitan un proveedor de acceso a Internet. En informática, se llama usuario en general, a todo persona que se encuentra usando un ordenador.



TÉRMINOS TÉCNICOS EN GENERAL

Abstract. Resumen de un documento donde se concretan sus características fundamentales a través de un proceso computacional.

Algoritmo. "Conjunto de instrucciones que cumplidas en el orden en que son enunciadas, conducen a la solución del problema, al cabo de un número determinado de pasos". [“Larousse. Gran Diccionario de las Ciencias”. Tomo 1. Ediciones Larousse, Barcelona-España, 1987, pág. 126.]

Algoritmo hash, de comprensión, destilación, de huella digital o de función resumen. Algoritmos que se aplican sobre determinado texto creando un resumen del mismo llamado hash.

Antivirus. Programas que protegen y eliminan o inutilizan virus.

Archivo. Unidad mínima de información organizada.

Banco de datos. Se pueden equiparar a los ficheros de una biblioteca especializada; proporcionan información o programas accesibles a los usuarios por medios informáticos. Dentro de los bancos de datos que se usan en el procesamiento de documentos jurídicos podemos señalar: el Batch, los on-line, los on-line evolucionados, los sistemas expertos, el OBAR, el IBM-TEXT PAC, y el STAIRS.

Binario. Compuesto de dos aspectos, en este caso de dos números, el cero y el uno. Lo que funciona con la numeración binaria.

Call Back Systems. Sistemas de control de acceso remoto al sistema (a través de módem). Una vez recibido y aceptado un código determinado el módem cuelga y llama al teléfono registrado como el del lugar donde se encuentra la terminal que tiene derecho a entrar en ese sistema.

CD-WORM (Write Once Read Many). Disco compacto en el que los datos sólo pueden ser almacenados en una ocasión, pero se pueden consultar tantas veces como se desee.

Chequera electrónica, billetera electrónica o monedero electrónico. Medio en el que se reservan valores y que tienen como base a una tarjeta inteligente.

Chip. Microcircuito integrado a una placa de silicio.

Cibernética. Rama de la ciencia que estudia los procesos de comunicación y de control automáticos en los sistemas, bien sea que se trate de conjuntos o de individuos formados por máquinas, organismos biológicos o sistemas sociales. [Padilla Segura, José Antonio. “Informática Jurídica”. SITESA, México, 1991, pág. 54.]

Cifrador. Algoritmos que permiten la ocultación de datos a través de la sustitución de letras o grupos de letras, e incluso del cambio del orden preestablecido de las mismas.

Cinta magnética. Tira de metal o de plástico con granitos de óxido ferromagnético en la que se guarda información.

Circuito. Sistema de conductores con entradas y salidas donde se transmiten impulsos que forman determinadas combinaciones. Esencialmente se dividen en circuitos ordinarios y circuitos integrados, los primeros son aquellos que adquieren una denominación determinada respondiendo al material de sus componentes principales que se encuentran fijos a una base y conectados ente sí por medio de hilos conductores, por ejemplo aquellos formados con transistores son denominados circuitos transistores. Los segundos se encuentran formados con componentes cuyas dimensiones son microscópicas, en ellos se fabrican todos los componentes al mismo tiempo, yuxtapuestos por millares sobre una laminilla de silicio.

Clave privada. Conjunto de datos únicos e inalterables generados en base a un procedimiento informático que garantiza su irreproducibilidad y confidencialidad, permitiendo firmar digitalmente con ella. [Proyecto de Ley sobre Documentos Electrónicos de la República de Chile. Ob. cit. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>]

Clave pública. Es el conjunto de datos únicos e inalterables generados en forma simultánea con la llave privada, que se corresponde unívocamente a los datos contenidos en ésta última, por lo que se emplea para verificar la clave privada. [Proyecto de Ley sobre Documentos Electrónicos de la República de Chile. Ob. cit. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>]

Clipper, Encriptación en custodia. Algoritmo simétrico clasificado que se usa para el control de la transmisión de información.

Código. En criptografía es la equivalencia entre símbolos comunes como letras y números con aquéllos ininteligibles por los cuales se les reemplaza. En informática, en general, son reglas establecidas de común acuerdo entre aquellos que diseñan los sistemas, entre ellos encontramos:

ISO (Organización Internacional de Estándares).

BCD (Código Binario Decimal), y

ASCII (Código Estándar Americano para Intercambio de Información).

Código secreto. Combinación de cifras y/o letras tecleadas haciendo uso de un determinado sistema.

Compatibilidad. En materia de informática se refiere a la afinidad de información entre diversos elementos informáticos como puede ser entre dos o más computadoras, o entre

computadoras y sus respectivos periféricos, siempre que manejen similares códigos y software.

Contraseñas, password, clave. Señal secreta que permite el conocimiento entre ciertas personas.

Contratación electrónica. Aquella que utiliza como medio o herramienta para transmitir declaraciones de voluntad de las partes contratantes la comunicación informática o telemática, independientemente de que el objeto de la contratación sea informático o no; siendo una de sus características el que la información enviada y recibida no está soportada en papel. [Carvajal Higuera, Luis Alfonso. Ob. cit. Disponible [Online]: <<http://emn.derecho.uma.es/obec/abstracts/ab333Carvajal.htm>>]

Controles de paridad y de disparidad. Programas en los que a los bit que componen un carácter se agrega un bit suplementario magnetizado si es par (control de paridad; viceversa si la técnica adoptada es la de control de disparidad), para que posteriormente el ordenador compare los bit suplementarios y conozca si ha existido alguna transformación en el cálculo.

Control de paridad/disparidad longitudinal. En estos programas además del control de paridad/disparidad sobre cada carácter, se efectúa un control ulterior de todos los bit que tienen la misma posición dentro de los caracteres transferidos como un bloque unitario.

Corrección de errores. Consiste en un software que asegura que los datos usados sean correctos, para ello el sistema corrige los errores manejando la corrección como una transacción separada que es grabada y contabilizada.

Convenio o contrato informático. “Acuerdo de partes en virtud del cual se crean, conservan, modifican o extinguen obligaciones relativas a los sistemas, subsistemas, o elementos destinados al tratamiento especializado de la información”. [Téllez Valdés, Julio. “Contratos, Riesgos y Seguros Informáticos”. Universidad Nacional Autónoma de México-Instituto de Investigaciones Jurídicas, primera edición, México, 1988, pág. 17.]

Criptografía. Técnica que utilizando algoritmos transforma, encripta o cifra la información legible en una ilegible usando un procedimiento y una clave determinada, y vuelve a hacer legible la información hasta que se aplique el mismo procedimiento y una clave secreta para desencriptarlo. Existen principalmente dos clases de criptografía:

La criptografía simétrica o sistemas de criptografía de clave privada o de clave secreta. Donde se usa la misma clave para encriptar y desencriptar el mensaje. Y la **criptografía asimétrica, de clave pública o RSA,** en la que se utilizan dos claves, una pública y otra privada.

Delito informático. Actitudes ilícitas en que se tienen a las computadoras como instrumento o fin. [Téllez Valdés, Julio. “Derecho Informático”. Ob. cit., pág. 105.]

Digesto seguro. Corresponde al hash.

Digital. Se refiere a toda computadora o proceso en el que los datos se representen por el paso de una corriente eléctrica.

Dinero digital, dinero electrónico, Electronic Money, E-cash, E-money. Esquema de pago por parte del cuentahabiente de un banco o institución financiera que integra en una tarjeta inteligente moneda virtual con moneda real. [Barrios Garrido, Gabriela; et al.. Ob. cit., pág. 66.] Dentro de los sistemas de dinero digital se encuentran Digicash, Netcash, E-cash, Cybercash y Mondex.

Documento electrónico, documento informático, documento magnético, o documento digital. En sentido estricto es 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, y que consiste en mensajes digitalizados que requieren de máquinas traductoras para ser percibidos y comprendidos por el hombre; y en sentido amplio los documentos electrónicos son aquéllos caracterizados por la posibilidad de ser percibibles y legibles directamente por el hombre sin necesidad de la intervención de máquinas traductoras. [Herrera Bravo, Rodolfo. "El documento electrónico: algunas vías de aplicación en el Derecho Probatorio Chileno". REDi: Revista Electrónica de Derecho Informático. Número 7, febrero, 1999. Disponible [Online]: <<http://derecho.org/redi/>>]

Encriptar o cifrar. Función a través de la cual datos legibles se transforman en datos ilegibles.

Enrutamiento diverso. Se envían los mensajes separados en partes y/o por diversos medios.

Espectro. Sucesión ordenada de las longitudes de onda o de frecuencia que intervienen en un fenómeno electromagnético, acústico, etc.. ["Larousse. Gran Diccionario de las Ciencias". Tomo 2. Ediciones Larousse, Barcelona-España, 1987, pág. 399.]

Fedd back o retroacción. Teoría que se basa en el uso de la retroalimentación de la información y de la relación máquina-hombre.

Firma electrónica, firma digital. Valor numérico que se adhiere a un mensaje transformándolo, y que permite mediante un procedimiento matemático, determinar si dicho mensaje corresponde a su autor manifiesto y si no se ha efectuado alguna modificación después de que el valor ha sido asignado a dicho mensaje. [Proyecto de Ley No.227 de abril 21 de 1998, por medio del cual se define y reglamenta el acceso y el uso del comercio electrónico, firmas digitales y se autorizan las entidades de certificación. Colombia. Disponible [Online]: <http://www.qmw.ac.uk/tl6345/colombia_sp.htm>]

Flujo de Datos Transfronterizos. "Circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y recuperación". [Definición

del Consejo Económico de la ONU citado por Téllez Valdés, Julio. "Derecho Informático". Ob. cit., pág. 77.]

Hackers. Terceros que obtienen con diversos fines un acceso no autorizado a un sistema de cómputo.

Hash, hash value o hash result. Resumen de un texto que consiste en un extracto de longitud fija de bits específico para ese mensaje, lo que permite la comparación entre éste y el obtenido posteriormente mediante la aplicación del algoritmo de comprensión, para determinar si el texto ha sido alterado.

Heurística. Método de inferencias lógicas aplicado a la inteligencia artificial.

Información inteligente o know how. Información útil y con posibilidades de aplicación.

Informática. Ciencia que forma parte de la cibernética y se encarga del estudio de los medios y mecanismos para transformar información aplicando las técnicas del tratamiento racional y automático; o ciencia del tratamiento automatizado de la información.

Informática jurídica o jurismática. Abarca la aplicación de la informática al tratamiento de la información jurídica. Se clasifica en informática jurídica documental, informática jurídica de control y de gestión, e informática jurídica metadocumental.

Instrucción o comando. Órdenes que en su conjunto forman programas y sistemas operativos y que indican a la computadora la acción a realizar.

Derecho de la informática. Comprende los aspectos normativos del uso de la informática.

Derecho informático. Rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (Derecho de la informática). [Téllez Valdés, Julio. "Derecho Informático". Ob. cit., pág. 22.]

Inteligencia artificial. Estudio de facultades mentales a través del uso de modelos computacionales. [Charniak y McDermott citados por Ríos Estavillo, Juan José. Ob. cit., pág. 63.]

Isomorfismo. Identidad entre dos sistemas, con partes relacionadas entre ellas sin alterar el todo.

Lápis óptico o penop. Instrumento que a través de electrones y rayos catódicos permite la representación de datos.

Llave o clave. Aplicados a la criptografía, son cadenas de bits relativamente cortas que controlan la salida del algoritmo, por lo que si cambia la llave cambia la salida del algoritmo.

Magnético. Que tiene propiedades de imán.

Microprocesador. Chip que efectúa las funciones de un procesador central completo.

Monitoreo electrónico. Sistema de control u observación efectuado por medios informáticos.

Nodo. Parte de una red en el cual convergen varios conductores.

On-line o En-línea. Estado que se da cuando varios módems se conectan y se encuentran listos para intercambiar datos.

Protocolo. En informática protocolo es el conjunto de reglas que permiten a una persona con los conocimientos técnicos necesarios, el conectar sus equipos a una red. [“Larousse. Gran Diccionario de las Ciencias”. Tomo 5. Ediciones Larousse, Barcelona-España, 1987, pág. 903.]

Red. Conjunto de computadoras interconectadas que permiten la comunicación entre las terminales y la central y viceversa, así como entre las terminales; con ello proporcionan a los usuarios la posibilidad de compartir información y equipo.

Respaldo. Medio de protección en caso de pérdida de información.

Revolución Digital o Revolución Informática. Fenómeno que ha transformado al mundo y se ha caracterizado por el incremento constante en la necesidad de información, lo que ha conllevado al desarrollo e incorporación de la informática en las actividades humanas.

Secure HyperText Transfer Protocol (SHTTP). Canal seguro de comunicación que se aplica a las conexiones HTTP.

Secure Socket Layer (SSL de Netscape) y Protocolo de Microsoft (PCT). Ambos encriptan las sesiones de comunicaciones y certifican digitalmente la identidad del vendedor.

Sellos del software. Protegen a los programas gracias a que el ordenador asocia a cada instrucción o serie de ellas un valor numérico, si el programa se modifica el valor de todas las instrucciones que lo componen se altera, y el programa rechaza la orden dada.

Sistema. Conjunto de reglas o principios así como de medios y técnicas para formar un todo homogéneo necesario para el funcionamiento de un ordenador.

Sistema biométrico. El ordenador utiliza características físicas del ser humano que son infalsificables, para efectuar la identificación de una persona.

Sistema de pago electrónico. Medio de pago que se realiza a través de medios tecnológicos.

Sistemas expertos. Se caracterizan especialmente por su capacidad de aprender. Realizan operaciones lógicas sobre una base de datos estructurada, a través de inferencias obtiene conclusiones. Un ejemplo de ellos es el Taxman II.

Sistema o Protocolo de Transacciones Electrónicas Seguras (SET: Secure Electronic Transaction). Sistema de criptografía desarrollado por Visa y Mastercard International para operar o realizar pagos en redes abiertas. Utiliza tanto el sistema de criptografía asimétrica como el de criptografía simétrica.

Slot. Hendidura perteneciente a un dispositivo de memoria y que permite la entrada de algún soporte de datos.

Soporte informático. Superficie que sirve de base para grabar datos, dependiendo del material de sus componentes puede ser magnético, u óptico, entre otros. Ejemplos de soportes informáticos lo constituyen el disquete y el CD-ROM.

Tarjeta inteligente, Smart card, Pc card. Tarjeta que cuenta con un chip que contiene un sistema operativo, programas de aplicación, y su propia memoria, lo que le permite almacenar valores y diversos datos, así como llevar un control estricto de los mismos.

Tarjeta magnética. Medio de almacenamiento en el que los datos se representan por medios magnéticos.

Tarjeta perforada. Medio de almacenamiento en el que las perforaciones o agujeros representan datos y el conjunto de ellos se convierten en información.

TEDI (Transferencia Electrónica de Datos Informatizados -en inglés EDI: Electronic Data Interchange). Intercambio de datos en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales. Las transacciones EDI se realizan sin papeles, utilizando para ello las redes de telecomunicación suministradas por los servicios públicos o privados o mediante servicios de Redes de Valor Agregado. [Devoto, Mauricio; Lynch, Horacio M.. "Banca, comercio, moneda electrónica y la firma digital". REDI: Revista Electrónica de Derecho Informático, número 2, septiembre, 1998. Disponible [Online]: <<http://derecho.org/redi/>>]

Teleinformática o telemática. Conjuga a la informática y a las telecomunicaciones permitiendo la transmisión de información procesada a distancia.

Terceras Partes Confiables o Autoridades de Certificación (TTP's: Thrusted Third Parties o CA: Certification Authorities). Tercero confiable que acredita la identidad de aquél que aparece en un certificado y el nexo entre éste y una determinada clave.

Texto cifrado o texto cripto. Escrito ilegible después de la aplicación de la criptografía.

Texto plano o texto claro. Escrito legible.

Tiempo de espera en la Terminal (Terminal Timeout). Si después de un tiempo predeterminado no se registra ninguna actividad en la terminal o estación de trabajo se cierra la sesión automáticamente.

Unidades de medida. En los sistemas informáticos son:

Bit (dígito binario). Es la unidad que representa la cantidad mínima de información que una computadora puede procesar, pudiendo tomar el valor de 0 (apagado) ó 1 (encendido).

Byte. Se conforma con ocho bits, es decir por una combinación de unos y ceros (por ejemplo: 01100110) y representan un carácter (letra, número o símbolo).

Kilobyte (K). Equivale a 1024 bytes.

Megabyte (MB). Equivale a 1024 kilobytes.

Gigabyte (GB). Equivale a 1024 megabytes.

Terabyte (TB). Equivale a 1024 gigabytes.

Vault Registry o certificado digital de la IBM. Garantiza las transacciones electrónicas con tecnología de identificación de los usuarios que realicen negocios electrónicos o e-business.

Virtual. Con existencia aparente.

Virus. Miniprogramas que dañan o destruyen información contenida en medios informáticos.

BIBLIOGRAFÍA Y HEMEROGRAFÍA

- AGUILERA FLORES, Margarita. "Urge verdadera política informática de Estado". El Universal, Universo de la Computación, lunes 17 de mayo de 1999, pág. 11.
- BARRIOS GARRIDO, Gabriela; MUÑOZ DE ALBA M., Marcia; PÉREZ BUSTILLO, Camilo. "INTERNET y Derecho en México". McGraw-Hill, primera edición, México, 1997, 180 págs..
- BORJA SORIANO, Manuel. "Teoría General de las Obligaciones". Porrúa, 13a. edición, México, 1994, 732 págs..
- BRENNA, Ramón Geronimo. "El 'documento digital': ¿La extinción de los papeles?". REDI: Revista Electrónica de Derecho Informático, número 1, agosto, 1998. Disponible [Online]: <<http://derecho.org/redi/>>
- CACHÓN BLANCO, José Enrique; ALONSO BALLESTEROS, Pilar. "Como hacer un contrato. Cien preguntas clave y sus respuestas". Dykinson, S.L., segunda edición, Madrid, 1995, 226 págs..
- CARNELUTTI, Francesco. "La prueba civil. Cómo nace el derecho. Cómo se hace un proceso". Tribunal Supremo de Justicia del D.F., México, 1993, 403 págs..
- CARVAJAL HIGUERAS, Luis Alfonso. "OBEC'97 Overcoming Barriers to Electronic Commerce". Disponible en línea: <<http://emn.derecho.uma.es/obec/abstracts/ab333Carvajal.htm>>
- CORNELLA, Alfons. "Información Digital para la Empresa". Marcombo. España, 1996, 180 págs..
- COUTURE, Eduardo J.. "Estudios de Derecho Procesal Civil". Tomo II. Depalma, Argentina, 1989, 478 págs..
- DEVOTO, Mauricio; LYNCH, Horacio M.. "Banca, comercio, moneda electrónica y la firma digital". REDI: Revista Electrónica de Derecho Informático, número 2, septiembre, 1998. Disponible [Online]: <<http://derecho.org/redi/>>
- DOMÍNGUEZ MARTÍNEZ, Jorge Alfredo. "Derecho Civil. Parte General, Personas, Cosas, Negocio Jurídico e Invalidez". Porrúa, tercera edición, México, 1992, 701 págs..
- "Enciclopedia Salvat". Tomo 2. Salvat editores, España, 1976, 1170 págs..
- "Enciclopedia Salvat". Tomo 4. Salvat editores, España, 1976, 1160 págs..

"Enciclopedia Salvat". Tomo 5. Salvat editores, España, 1976, 1448 págs..

ESCALANTE, Alejandro. "¿Qué es la Internet?". Disponible [Online]: <<http://www.insp.mx/salvia/978/Sal9784.html>>

FIX FIERRO, Héctor. "Informática y Documentación Jurídica". UNAM, segunda edición, México, 1996, 116 págs..

GARCÍA AGUILAR, Nicolás. "La cuestión de la responsabilidad en el Derecho Informático". REDI: Revista Electrónica de Derecho Informático. Disponible [Online]: <<http://derecho.org/redi/>>

GARCÍA MÁYNEZ, Eduardo. "Introducción al Estudio del Derecho". Porrúa, cuadragésimo cuarta edición, México, 1992, 444 págs..

GÓMEZ LARA, Cipriano. "Derecho Procesal Civil". Harla, quinta edición, México, 1994, 441 págs..

GORE, Al. Transcripción de las palabras que el Vicepresidente de los Estados Unidos dirigió el 1º de julio de 1997 en ocasión del informe a la Casa Blanca sobre la Estructura del Comercio Electrónico. Cuestiones Mundiales, Publicación Electrónica del Usis, volumen 2, octubre, 1997. Disponible [Online]: <<http://www.usia.gov/journals/itgic.htm>>

GRAHAM-ALCANTARA, James A.. "¿Hacia una obligación de resultado en materia de seguridad de redes?". REDI: Revista Electrónica de Derecho Informático, número 7, febrero, 1999. Disponible [Online]: <<http://derecho.org/redi/>>

HANCE, Olivier. "Leyes y Negocios en Internet". Traducción de Yazmín Juárez Parra. McGraw-Hill, México 1996, 371 págs..

HERNÁNDEZ, Luis Antonio. "Internet y Legislación. Comercio electrónico, una tarea incompleta". El Universal, Universo de la Computación, lunes 17 de mayo de 1999, pág. 9.

HERNÁNDEZ, Luis Antonio. "Internet y Legislación. Comercio electrónico y desarrollo social". El Universal, Universo de la Computación, lunes 28 de junio de 1999, pág. 9.

HERNÁNDEZ, Luis Antonio. "Internet y Legislación. Derecho digital mexicano". El Universal, Internet-Universo de la Computación, lunes 24 de mayo de 1999, pág. 4.

HERRERA BRAVO, Rodolfo. "El documento electrónico: algunas vías de aplicación en el Derecho Probatorio Chileno". REDI: Revista Electrónica de Derecho Informático, número 7, febrero, 1999. Disponible [Online]: <<http://derecho.org/redi/>>

"Informática y Derecho. Aportes de Doctrina Internacional". Director ALTMARK, Daniel R.. Depalma, reimpresión, Buenos Aires, 1991, Volumen 1, 176 págs..

“Informática y Derecho. Aportes de Doctrina Internacional”. Director ALTMARK, Daniel R.. Depalma, reimpresión, Buenos Aires, 1993, Volumen 4, 208 págs..

IRIARTE AHON, Erick. “Violencia en Internet, ¿Quién defiende a los Internautas?. Sobre el abuso del Correo Electrónico”. REDI: Revista Electrónica de Derecho Informático, número 6, enero, 1999. Disponible [Online]: <<http://derecho.org/redi/>>

JIJENA LEIVA, Renato Javier. “Comercio electrónico y Derecho. La problemática jurídica del Comercio Electrónico”. REDI: Revista Electrónica de Derecho Informático, número 9, abril, 1999. Disponible [Online]: <<http://derecho.org/redi/>>

“Jurisprudencia y Tesis Aisladas 1917-1998”. Suprema Corte de Justicia de la Nación. IUS 8.

KEMPER, Ana María. “XXIV Jornada Notarial Argentina, Buenos aires, octubre 1996. Tema I. Seguridad en la contratación por medios electrónicos. Documento electrónico”. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

LANE, J.E.. “Telemática y Comunicaciones en la Empresa”. Paraninfo. España, 1986, 124 págs..

“Larousse. Gran Diccionario de las Ciencias”. Tomo 1. Ediciones Larousse, Barcelona-España, 1987, 192 págs..

“Larousse. Gran Diccionario de las Ciencias”. Tomo 2. Ediciones Larousse, Barcelona-España, 1987, 400 págs..

“Larousse. Gran Diccionario de las Ciencias”. Tomo 4. Ediciones Larousse, Barcelona-España, 1987, 800 págs..

“Larousse. Gran Diccionario de las Ciencias”. Tomo 6. Ediciones Larousse, Barcelona-España, 1987, 1197 págs..

LEVINE, John R.; BAROUDI, Carol. “Internet para Inexpertos”. Editorial Limusa, primera reimpresión, México, 1996, 438 págs..

MARTÍNEZ FAZZALARI, Raúl. “Proyecto de Ley de Exención Impositiva para las Transacciones Comerciales por Internet”. REDI: Revista Electrónica de Derecho Informático, número 5, diciembre, 1998. Disponible [Online]: <<http://derecho.org/redi/>>

“Master Informática. Manejo del PC y MS-DOS 5.0”. F&G editores, Madrid, 1992, 207 págs..

- ORTECHO, José Manuel. "Dominios en Internet. ¿Qué son?". REDI: Revista Electrónica de Derecho Informático, número 3, octubre, 1998. Disponible [Online]: <<http://derecho.org/redi/>>
- OVALLE FAVELA, José. "Derecho Procesal Civil". Harla, séptima edición, México, 1995, 400 págs..
- PADILLA SEGURA, José Antonio. "Informática jurídica". SITESA, primera edición, México, 1991, 170 págs..
- PALADELLA SALORD, Carlos. "Datos Personales Contenidos en Bases de Datos y Registros Electrónicos". REDI: Revista Electrónica de Derecho Informático. Disponible [Online]: <<http://derecho.org/redi/>>
- PALADELLA SALORD, Carlos. "El dinero físico y su desaparición?". REDI: Revista Electrónica de Derecho Informático, número 10, mayo, 1999. Disponible en línea: <<http://derecho.org/redi/>>
- "Periódico ABZ, Información y Análisis Jurídicos. Anuario 1998." ABZ editores, primera edición, México, 1998, 600 págs..
- PRADO, Pedro Antonio. "La Informática y el Abogado". Abeledo-Perrot. Argentina, 1988, 130 págs..
- "Primera consulta documental sobre el desarrollo del Internet en México". Comisión Federal de Telecomunicaciones, México, 23 de junio, 1997. Disponible [Online]: <<http://www.nic.mx/news/consulta.html>>
- PINA, de Rafael; PINA VARA, de Rafael. "Diccionario de Derecho". Porrúa, vigesimoprimera edición, México, 1995, 525 págs..
- RABASA, Emilio O.; CABALLERO, Gloria. "Mexicano: ésta es tu Constitución". Miguel Ángel Porrúa, decimoprimera edición, México, 1997, 435 págs..
- RAMOS SUÁREZ, Fernando. "La firma digital". REDI: Revista Electrónica de Derecho Informático, número 9, abril, 1999. Disponible [Online]: <<http://derecho.org/redi/>>
- RAMOS SUÁREZ, Fernando. "Leyes que gobiernan Internet y normativas legales a aplicar en un entorno donde no existen fronteras geográficas". REDI: Revista Electrónica de Derecho Informático, número 10, mayo, 1999. Disponible [Online]: <<http://derecho.org/redi/>>
- RAMOS SUÁREZ, Fernando. "Seguridad en la venta de un producto por Internet". REDI: Revista Electrónica de Derecho Informático, número 4, noviembre, 1998. Disponible [Online]: <<http://derecho.org/redi/>>

RIBAS, Xavier. "Comercio electrónico en Internet. Aspectos jurídicos". REDI: Revista Electrónica de Derecho Informático, número 1, agosto, 1998. Disponible [Online]: <<http://derecho.org/redi/>>

RIBAS, Xavier. "Propuesta de Directiva sobre firmas electrónicas". REDI: Revista Electrónica de Derecho Informático, número 2, septiembre, 1998. Disponible [Online]: <<http://derecho.org/redi/>>

RIESTRA, Eduardo. "El autor en el ciberespacio". REDI: Revista Electrónica de Derecho Informático, número 7, febrero, 1999. Disponible [Online]: <<http://derecho.org/redi/>>

RÍOS ESTAVILLO, Juan José. "Derecho e Informática en México". UNAM, primera edición, México, 1997, 175 págs..

RODRÍGUEZ, Luis Angel. "Seguridad de la información en sistemas de Cómputo". Ventura ediciones, México, 1995, 353 págs..

TÉLLEZ VALDEZ, Julio. "Contratos, Riesgos y Seguros Informáticos". Universidad Nacional Autónoma de México-Instituto de Investigaciones Jurídicas, primera edición, México, 1988, 253 págs..

TÉLLEZ VALDES, Julio. "Derecho Informático". McGraw-Hill, segunda edición, México, 1997, 283 págs..

TREJO DELARBRE, Raúl. "La nueva alfombra mágica. Usos y mitos de Internet, la red de redes". Disponible [Online]: <<http://www.etcetera.com.mx/libro/alfombra.htm>>

VARELA DORBECKER, Jorge. "Tiempo de Decisión. ¡Proteja su Información!". El Universal, Universo de la Computación, lunes 15 de marzo de 1999, pág. 6.

VELARDE KOEHLIN, Carmen. "El fedatario particular juramentado en informática: Institución peruana al servicio de una solución global". REDI: Revista Electrónica de Derecho Informático, número 8, marzo, 1999. Disponible [Online]: <<http://derecho.org/redi/>>

WITKER, Jorge; JARAMILLO, Gerardo. "Comercio Exterior de México, Marco Jurídico y Operativo". McGraw-Hill. México, 1997, 189 págs..

ZAGO, Jorge Alberto. "El consentimiento en los contratos y la teoría de la lesión". Editorial Universidad, Argentina, 1981, 216 págs..

ZAMORA Y VALENCIA, Miguel Angel. "Contratos Civiles". Porrúa, Quinta edición, México, 1994, 444 págs..

“IX Jornada Notarial de América del Norte, Centroamérica y el Caribe. Informe sobre la contratación por vía electrónica en la Argentina”. Puerto Rico, septiembre, 1997. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

“XXIV Jornada Notarial Argentina. Tema I. Seguridad jurídica en la contratación por medios electrónicos. Documento electrónico -considerando-”. Argentina, Buenos Aires, octubre, 1996. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

LEGISLACIÓN

Borrador del Proyecto de Ley de Firma Digital Alemana (SigG). Traducción y comentarios por KURNER, Chistopher. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

Código Civil para el Distrito Federal.

Código de Comercio.

Código de Procedimientos Civiles para el Distrito Federal.

Decreto No. 427, Argentina, Buenos Aires, 16 de abril de 1998. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

Fisco Agenda 98.

Legislación mexicana. InfoJus WWW. Disponible [Online]: <<http://www.juridicas.unam.mx/legislac/>>

Ley de Comercio Minorista. Ventas a distancia. Ley 7, 15 de enero de 1996, BOE 17 de enero de 1996. Disponible [Online]: <<http://www.onnet.es/leyes.htm>>

Ley del Notariado para el Distrito Federal.

Ley Federal de Protección al Consumidor.

Proyecto de Ley No. 227, de Colombia del 21 de abril de 1998, por medio del cual se define y reglamenta el acceso y uso del comercio electrónico, firmas digitales y se autorizan las entidades de certificación. Disponible [Online]: <http://www.qmw.ar.uk/tl6345/colombia_sp.htm>

Proyecto de Ley sobre Documentos Electrónicos de la República de Chile. CENIT: Centro de Investigaciones en Information Technology-Estudio Jara, Del Favero y Cía. Disponible [Online]: <<http://www.sfp.gov.ar/firma.html>>

Tratado de Libre Comercio de América del Norte. Disponible [Online]: <http://www.sice.oas.org/Trade/nafta_s/indice1.STM>

ÍNDICE

INTRODUCCIÓN

CAPÍTULO I. LA REVOLUCIÓN DIGITAL. 1

1.1. La cibernética.....	1
1.2. Las computadoras.....	4
1.2.1. Historia y desarrollo.....	4
1.2.2. Concepto.....	6
1.3. La informática.....	7
1.3.1. La teleinformática.....	9
1.4. Internet.....	9
1.4.1. Antecedentes.....	11
1.4.2. Funcionamiento.....	13
1.4.2.1. Sistema de Nombre de Dominio.....	14

CAPÍTULO II. LA INFORMÁTICA Y EL DERECHO. 17

2.1. Informática jurídica o jurismática.....	17
2.1.1. Historia.....	18
2.1.2. Contenido, concepto y clasificación.....	19
2.1.2.1. Informática jurídica documental.....	20
2.1.2.2. Informática jurídica de control y/o gestión.....	22
2.1.2.3. Informática jurídica metadocumental.....	22
2.1.3. Informática legislativa y judicial.....	24
2.2. El Derecho de la informática.....	26
2.3. Normatividad de la informática en México.....	28
2.3.1. Marco normativo de la informática en nuestro país.....	28
2.4. Flujo de Datos Transfronterizos (FDT).....	34
2.4.1. Marco jurídico de Internet en los Estados Unidos Mexicanos.....	36

CAPÍTULO III.

EL DOCUMENTO ELECTRÓNICO. 40

3.1. El documento electrónico como documento escrito.....	42
3.2. Elaboración del documento electrónico.....	45
3.3. Características del documento electrónico.....	47
3.3.1. Criptografía.....	57
3.3.1.1. Funcionamiento de la criptografía.....	59
3.3.1.2. Exportación de la criptografía.....	61
3.4. El documento electrónico como documento jurídico.....	63
3.4.1. El documento jurídico digital.....	65
3.4.1.1. Documentos materiales y literales.....	67
3.5. El documento heterógrafo.....	72
3.6. El documento autógrafo.....	72
3.7. La firma electrónica.....	73
3.8. Conveniencia de la intervención notarial en la documentación electrónica.....	83
3.8.1. El Proyecto del Cibernotario.....	85
3.9. El documento electrónico como medio de prueba.....	86

CAPÍTULO IV.

LA CONTRATACIÓN ELECTRÓNICA. 89

4.1. La etapa precontractual.....	89
4.2. El contrato electrónico.....	90
4.2.1. La autonomía de la voluntad.....	91
4.2.2. El consentimiento.....	91
4.2.2.1. La oferta y la aceptación.....	92
4.2.3. El objeto.....	95
4.2.4. La forma.....	95
4.2.5. El rol del Notario.....	99
4.3. Sistemas de pago electrónicos.....	100

CAPÍTULO V.
MARCO NORMATIVO DEL DOCUMENTO ELECTRÓNICO EN
MÉXICO.

106

5.1. Implementación del documento electrónico.....	106
5.1.1. Ventajas económicas y sociales.....	113
5.1.2. Aspectos positivos de la regulación jurídica del documento electrónico.....	115
5.2. Reconocimiento legal del documento electrónico como forma de contratación....	116
5.2.1. Análisis de los artículos 1832, 1833 y 1834 del Código Civil para el Distrito Federal y propuesta de reformas.....	117

CONCLUSIONES.....	119
--------------------------	------------

GLOSARIO

Términos básicos sobre la estructura y el funcionamiento de las computadoras....	121
Términos básicos sobre la estructura y el funcionamiento de Internet.....	124
Términos técnicos en general.....	126

BIBLIOGRAFÍA Y HEMEROGRAFÍA.....	134
---	------------

LEGISLACIÓN.....	140
-------------------------	------------