UNIVERSIDAD DE COSTA RICA

FACULTAD DE DERECHO

"ACTUACIONES NOTARIALES FORMADAS EN EL EXTRANJERO Y SUS APLICACIONES CIBERNÉTICAS"

(ACTUACIONES NOTARIALES ELECTRÓNICAS)

Tesis para optar al grado de Licenciatura en Derecho

KADIR CORTES PEREZ

2002

UNIVERSIDAD DE COSTA RICA
FACULTAD DE DERECHO
AREA DE INVESTIGACIÓN

San José, 30 de mayo del 2002.-

Dr.
Rafael González Ballar
Decano, FACULTAD DE DERECHO

Hago de su conocimiento que el Trabajo Final de Graduación del estudiante

KADIR CORTES PEREZ

Titulado: "***ACTUACIONES NOTARIALES FORMADAS EN EL EXTRANJERO Y SUS APLICACIONES CIBERNÉTICAS" (ACTUACIONES NOTARIALESS ELECTRÓNICAS***" fue aprobado por el Comité Asesor, a efecto de que el mismo sea sometido a discusión final. Por su parte, el suscrito ha revisado los requisitos de forma y orientación exigidos por esta Área y lo aprueba en el mismo sentido.

Asimismo le hago saber que el Tribunal Examinador quedó integrado por los siguientes profesores:

Presidente: LIC. JULIAN SOLANO PORRAS
Secretario: LIC. VICTOR RODRIGUEZ RESCIA
Informante: LIC. ROY JIMÉNEZ OREAMUNO
Miembro: LIC. WILLIAM BOLAÑOS GAMBOA
Miembro: LIC. GUSTAVO ADOLFO INFANTE MELENDEZ

La fecha y hora para la PRESENTACION PUBLICA de este trabajo se fijó para el día viernes 07 de junio del 2002, a las 11:00 a.m. horas.

Atentamente,

UNIVERSIDAD DE COSTA RICA
FACULTAD de DERECHO

DR. DANIEL GADEA NIETO
DIRECTOR
AREA DE INVESTIGACIÓN
FACULTAD DE DERECHO

Bufete Roy A. Jiménez O.

Tel. 223- 2114 *Fax 223- 3402* *e-mail: royji@yahoo.es*

San José, 15 de mayo del 2002.

Señor
Dr. Daniel Gadea Nieto
Director Área de Investigación
Presente

Por medio de la presente, me permito dar mi aprobación al trabajo de graduación realizado por el estudiante **KADIR CORTÉS PÉREZ**, carné 810865, intitulado: **"ACTUACIONES NOTARIALES FORMADAS EN EL EXTRANJERO Y SUS APLICACIONES CIBERNÉTICAS (ACTUACIONES NOTARIALES ELECTRÓNICAS)"**, el presente trabajo desarrolla la problemática existente del documento electrónico y la necesidad de aceptar la utilización del mismo en el ámbito notarial.

Enfoca la problemática jurídica de la utilización del documento informático, entre la cultura y legislación nuestra orientada al documento papel. La necesidad de las autoridades certificadoras para la utilización de firmas digitales. Y la participación notarial en algunos casos en que se requiera de acuerdo a la legislación del lugar en donde surtirá efecto jurídico dicho documento, la participación de un notario. Todo lo anterior, teniendo en cuenta la existencia de un proyecto de ley sobre firmas digitales y certificados digitales.

Este trabajo es desarrollado exhaustivamente, teniendo en cuenta lo novedoso del mismo, y lo acelerado del cambio en la tecnología informática, que se contrapone a lo conservador del ejercicio notarial, en el que únicamente se ha introducido la utilización de la máquina de escribir o de un computador como procesador de palabras en los últimos veinticinco años en la elaboración de documentos notariales.

Atentamente,

Lic. Roy A. Jiménez Oreamuno

Arch.

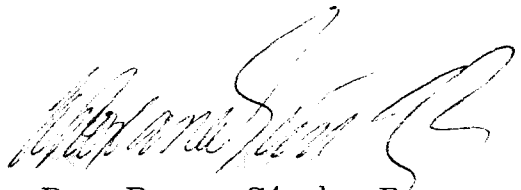
24 de mayo del 2002

Doctor
Daniel Gadea Nieto
Area de Investigación
Facultad de Derecho

Estimado Dr. Gadea:

La presente es para informarle que apruebo el trabajo en fondo y forma, realizado por el estudiante **KADIR CORTES PEREZ,** carné **810865**, titulado **"ACTUACIONES NOTARIALES FORMADAS EN EL EXTRANJERO Y SUS APLICACIONES CIBERNÉTICAS (ACTUACIONES NOTARIALES CIBERNÉTICAS)"**.

Atentamente,



Dra. Roxana Sánchez Boza

San José, 16 de mayo del 2002

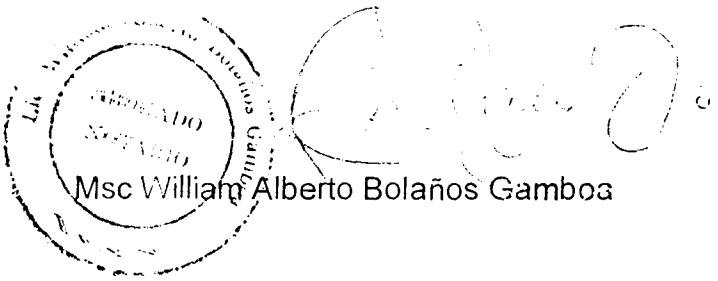
Señor
Daniel Gadea Nieto
Director Área de Investigación
Presente

Estimado Dr. Gadea:

Por medio de la presente me permito dar aprobación al trabajo de graduación realizado por el estudiante KADIR CORTÉZ PÉREZ, carné 810865, titulado "ACTUACIONES NOTARIALES FORMADAS EN EL EXTRANJERO Y SUS APLICACIONES CIBERNÉTICAS (ACTUACIONES NOTARIALES CIBERNÉTICAS)".

El trabajo hace un estudio del desarrollo del documento electrónico de las firmas digitales y su posible aplicación a la función notarial. La problemática del tema es actual tomando en cuenta que se encuentra en estudio de la Asamblea Legislativa un proyecto de ley sobre firmas digitales y certificados digitales y por el desarrollo de la tecnología informática en el país.

Atentamente



Msc William Alberto Bolaños Gamboa

Gracias Madre, que Dios te bendiga

Eres parte de mis logros y de este trabajo.

Ale, Jime, mi adoración e incentivo.

INDICE

FICHA BIBLIOGRAFICA:

CORTES PEREZ (Kadir) **"ACTUACIONES NOTARIALES FORMADAS EN EL EXTRANJERO Y SUS APLICACIONES CIBERNÉTICAS" (ACTUACIONES NOTARIALES ELECTRÓNICAS)**. Tesis para optar por el grado de Licenciado en Derecho, Facultad de derecho, Universidad de Costa Rica, San José, Costa Rica, 2002.

DIRECTOR: Lic. Roy Jiménez Oreamuno.

LISTA DE PALABRAS CLAVES: - Documento electrónico.

- Contrato Electrónico.
- Firma Digital.
- Autoridades Certificadoras.
- Notario Cibernético o Cibernotario.
- Protocolo Digital.

RESUMEN DEL TRABAJO:

Los usos de los nuevos recursos tecnológicos de comunicación y, por ende, de contratación, hacen necesario determinar por ley que el documento electrónico tiene plena validez legal y probatoria.

La firma digital es un medio de seguridad de los documentos electrónicos, la cual surge de un proceso que utiliza técnicas de criptografía de doble llave con una función matemática que verifica la titularidad del emisor del documento, otorgando autenticidad, confiabilidad, integridad y no repudio del mensaje.

El sistema de firma digital funciona bajo la existencia de las Autoridades de Certificación, quienes autentican digitalmente la identidad del titular de cada firma. Esta función no debe ser confundida con la autenticación legal, que en nuestro ordenamiento está reservada para los Abogados y Notarios.

El Notario tendrá un nuevo campo de acción en la contratación y actuación electrónica, ya que:

1- Será necesariamente el encargado de autenticar y dar fe de la identidad y capacidad de los usuarios ante las Autoridades Certificadoras.

2- Podrá certificar las firmas digitales de documentos electrónicos privados.

3- Será necesaria su firma digital, cuando por ley se requiera que un documento sea autenticado legalmente.

La participación del Notario ejercería un control de legalidad para la validez del contenido jurídico del documento, y dará fe pública de los procesos de certificación digital.

Para que el Notario realice su función en el ámbito electrónico, deberá estar capacitado para otorgar ese servicio, tener conocimientos suficientes en informática y en certificación digital, dando nacimiento a la figura del "Notario Cibernético".

Es interesante analizar como, a pesar de un dictamen de la Procuraduría General de la República, en nuestra legislación se han ido introduciendo normas que permiten el uso de documentos electrónicos y la utilización de ciertos elementos electrónicos de seguridad para ser utilizados como firma de dichos documentos. Esto no es saludable, pues no se debe legislar sobre firma digital para sus aplicaciones en algunas áreas, sino garantizar una apertura a todos los sectores de la sociedad.

Es necesario ir delineando la función de la Dirección Nacional de Notariado, quien deberá determinar la firma digital como un medio idóneo de seguridad de los documentos notariales electrónicos. El Registro Público únicamente deberá

reformar el artículo 57 de su Reglamento, para que se le permita tramitar documentos por medios tecnológicos.

Nuestra intención con el desarrollo de este tema, fue mostrar un poco la realidad del avance en la tecnología, la insuficiencia de nuestro ordenamiento, la soluciones encaminadas en otros países y la necesidad de legislar sobre firma digital.

INTRODUCCIÓN GENERAL

INTRODUCCIÓN

El avance en las nuevas tecnologías hacen que se dé un incremento en el intercambio de información por vía electrónica y que cada día su acceso sea más fácil para gran parte de la sociedad, constituyendo un movimiento destinado a producir cambios en la relaciones sociales y económicas.

Los Gobiernos están en la obligación de garantizar una infraestructura que dote de seguridad a ese tráfico de información que se realiza electrónicamente.

Por otro lado y atendida la circunstancia que nuestro país tiene un sistema de economía abierta , en la cual el comercio internacional juega un papel muy importante, es indispensable crear instrumentos que faciliten los intercambios internacionales.

Tecnológicamente, Costa Rica está preparada para el gran paso de la economía digital, mediante la Red Nacional de Internet de Alta Capacidad.

El Ministerio de Ciencia y Tecnología pretende desarrollar su proyecto denominado "gobierno digital", por el cual se daría soluciones más rápidas a las exigencias de los usuarios. Con dicho proyecto todos los trámites a realizar ante oficinas públicas podrán ser hechos en línea.

Lo anterior llevo al Gobierno de la República a presentar el Proyecto de Ley sobre Firmas y Certificados Digitales. Este Proyecto, aunque adolece de ciertas limitaciones, viene a introducir en nuestro ordenamiento jurídico un instrumento que facilitará el comercio y la contratación por medios electrónicos.

El fenómeno de la globalización, el comercio electrónico y la creciente contratación internacional entre sujetos de derecho privado, se ha pensado en formas de adaptar el derecho a esta constante evolución, por lo que debemos modernizar la función notarial de manera que otorgue mayor seguridad y certeza a esas relaciones jurídicas, dando lugar a la función notarial electrónica.

El objetivo general del presente trabajo es el análisis jurídico de la función notarial ante el avance de la tecnología electrónica.

Con ese fin, pretendemos determinar los fundamentos de la función notarial tradicional del sistema latino y su traslado a la contratación electrónica, pues el Notario Cibernético es un embrión de nuestro sistema de notariado.

Los objetivos específicos que nos propusimos para el desarrollo del tema son los siguientes:

1- Determinar la intervención de Notario ante las nuevas tecnologías de comunicación y contratación electrónica.

2- Analizar la supresión del principio de la unidad del acto notarial en la función notarial cibernética.

3- Determinara las condiciones se seguridad, las certificaciones de los documentos notariales informáticos, la validez de estos documentos como medio de prueba.

4- Analizar la figura del Notario Cibernético como el funcionario encargado de validar los contratos electrónicos.

5- Determinar las ventajas y desventajas de la función notarial electrónica.

El trabajo es un aporte inicial al estudio de la formación del contrato electrónico desde el punto de vista del Derecho Civil y de la función notarial electrónica, quedando abierta la investigación de la aplicación de la tecnología electrónica en actos y contratos en otros campos del derecho como es el derecho comercial, administrativo, etc.

Es además un aporte al análisis del avance que debe darse en la función notarial, como ejemplo de que el Derecho como ciencia social debe adaptarse lo más posible a la evolución del mundo moderno. El tema se torna polémico debido a que, por lo reciente, doctrinalmente no se le ha dado un trato extenso, no existen antecedentes judiciales y las legislaciones de otros países apenas inician su regulación.

Es por ello que será necesario recurrir a los artículos de revistas en la red Internet, a legislaciones modelo comúnmente utilizadas y a legislaciones de otros países que han iniciado su regulación.

Es por esa razón que se procederá a utilizar el método comparativo y deductivo de la situación actual del tema en la comunidad internacional, en relación con la situación de nuestra realizada nacional, especialmente tomando en cuenta el Proyecto de Ley de Firmas Digitales y Certificados Digitales.

Al finalizar el desarrollo de este trabajo pretendemos demostrar las hipótesis:

a) Que la función de los Notarios Públicos será importante en la autenticación legal de los usuarios en el sistema de autenticación digital que realizan las Autoridades de Certificación y para autenticar contratos realizados en el medio digital.

b) Que con la contratación electrónica se rompe el principio de la unidad del acto notarial, lo cual es necesario para adaptar la función notarial al avance de la electrónica.

c) Que el avance en los sistemas de comunicación, la tecnología electrónica y el crecimiento del comercio electrónico, hacen necesaria una legislación sobre criptografía, autenticación y certificación de documentos electrónicos, que

regularían todo lo referente a la transmisión de datos, documentos electrónicos, firmas digitales, entidades de certificación, entidades de registro, contratos electrónicos y la forma en que el Notario actuará en el ambiente digital.

d) Que los documentos electrónicos cumplen con los requisitos necesarios de validez, certeza, seguridad y autenticidad, por lo que es necesaria su aprobación legal para otorgarle pleno valor probatorio.

e) Que únicamente un especialista en Derecho Notarial, debidamente acreditado por sus conocimientos en informática, podrá actual como Notario Cibernético.

Este trabajo se divide en cuatro títulos guardando la simetría en sus capítulos en cuanto a los temas a tratar.

El primer título está referido al documento en general, donde el capítulo primero hace un análisis del documento notarial, sus elementos, clasificación y fines; se hace también un repaso de la fe pública notarial.

En el capítulo segundo tratamos las actuaciones notariales formadas en el extranjero, pues cada día los actos y contratos autorizados por nuestros Cónsules en el extranjero o por nuestros notarios nacionales en su actuación extraterritorial son más comunes, en razón del fenómeno de la globalización. Es necesario repasar

dichas actuaciones en atención a la aplicación de la tecnología y a la economía de tiempo que conllevaría realizar esas actuaciones de manera electrónica.

En razón de que el tema toca aspectos de la informática, el título segundo hace un análisis sobre la informática en general. En el capítulo primero tratamos el origen y la evolución de la red Internet, qué es y que servicios nos presta. Además desarrollamos temas desde el punto de vista informático, como el lenguaje o protocolos utilizados en Internet y de la seguridad en el tráfico de información.

Posteriormente, en el capítulo segundo iniciamos a tratar de establecer las nociones de la contratación electrónica, desde la óptica de la contratación civil, y de la formación del contrato electrónico.

El título tercero entra a desarrollar en tres capítulos la función notarial electrónica. Primero haremos un análisis del documento electrónico, ya que en este punto existe oposición del gremio de los Notarios en cuanto a la aceptación de los documentos informáticos y sobre todo a los documentos notariales informáticos.

Esta oposición está referida a las condiciones de seguridad, confiabilidad, integridad y autenticidad, que son necesarios para determinar la validez de los documentos electrónicos en relación con los documentos de papel, condiciones que serán tema de estudio.

De ahí se parte al análisis en el segundo capítulo de la firma digital y de la utilización de claves que sirven de medio de seguridad de las comunicaciones electrónicas. Posteriormente, en los siguientes dos capítulos y para determinar la autenticidad de dichas comunicaciones firmadas digitalmente, veremos lo referente a los Certificados Digitales y las Autoridades de Certificación y la discusión del presunto desplazamiento de la función notarial hacia estas entidades.

La figura del Notario Cibernético, como funcionario que certificará y validará los documentos y contratos electrónicos, es de análisis puntual en el título cuarto.

Estudiaremos en el capítulo primero cómo nace la figura en el Common Law y su traslado a los sistemas de notariado latino, como una necesidad de proveer seguridad jurídica a las transacciones internacionales realizadas por medios electrónicos. Es necesario que los profesionales en derecho conozcan esta nueva forma de la función notarial, los requisitos exigidos para ser un Notario Cibernético y la forma correcta de realizar dicha función.

El capítulo segundo tratará un tema muy polémico, como es la posibilidad del Protocolo Digital donde asentar los instrumentos notariales electrónicos.

Aunque pareciera que el tema es extraño en nuestro ordenamiento jurídico, en el capítulo tercero realizaremos un estudio de algunas normas vigentes que

reconocen validez y eficacia a los documentos electrónicos y a los caracteres electrónicos utilizados como firma en dichos documentos.

El papel de la Dirección Nacional de Notariado, como institución que determina la seguridad de los documentos notariales y del Registro Público, como institución encargada de inscribir los instrumentos públicos y de dar publicidad a las inscripciones, formarán parte del capitulo cuarto de este título.

Por el avance vertiginoso del tema en la Comunidad Europea, el desarrollo de los diferentes aspectos tomará en cuenta las Directivas del Parlamento Europeo y del Consejo y las diversas Propuestas de Directivas Europeas.

Es interesante lo dicho por un Abogado especializado en Derecho Informático y Tecnologías de la Información, antes de que se aprobará en España el Decreto Ley sobre el uso de la firma digital: " Todos los sujetos sociales se ven influenciados de alguna u otra forma por las nuevas tecnologías. Para nosotros los abogados se nos hace todavía más cuesta arriba, pues nos tenemos que subir a un tren que hace tiempo que ha salido. Si ya de por sí el legislador va por detrás de las conductas sociales, imaginemos como tiene que ir cuando la evolución tecnológica supera con mucho cualquier previsión o expectativa de futuro... Hay que subirse al tren por rápido que sea, o te subes o te quedas atrás. Quizás aquí los abogados jóvenes tenemos más ventaja que otros que ya han visto pasar por sus

ojos varias décadas. No obstante, creo que es necesario por parte de todos hacer un esfuerzo por adaptarse lo mejor posible a la nueva sociedad de la información."[1]

Si tecnológicamente estamos preparados, nuestra profesión debe hacer lo propio. En adelante, pretendemos dar algunas pautas para encender la discusión en esta materia, de tan poco tratamiento en el ámbito notarial de nuestro país.

[1] RAMOS SUAREZ (Fernando) La Firma Digital. Revista Electrónica de Derecho Informático. www.publicacion.derecho.org/redi, p. 1

TITULO PRIMERO:

EL DOCUMENTO EN GENERAL

CAPíTULO I:

EL DOCUMENTO NOTARIAL

Sección I: CONCEPTUALIZACION DEL DOCUMENTO.

Para determinar inicialmente los documentos notariales, es menester conocer la acepción general que se utiliza de documento. Así se define documento como: "Diploma, carta u otro escrito que ilustra acerca de algún hecho. Escrito donde se prueba una cosa". [1]

El documento es en sentido amplio, cualquier cosa que represente un hecho y si ese hecho es representado mediante la escritura, se llama documento en sentido estricto. [2]

En los documentos el autor exterioriza su pensamiento de un hecho y es así como nuestro Código Procesal Civil recoge una definición amplísima de documento cuando establece que: "Son documentos escritos, los impresos, los planos, los dibujos, los cuadros, las fotografías, las radiografías, las cintas cinematográficas, los discos, las grabaciones magnetofónicas y en general, todo objeto mueble que tenga carácter de representativo o declarativo."[3]

---

[1] Océano Uno Color, Diccionario Enciclopédico, Océano Grupo Editorial S.A., Barcelona, Edición 1998,. Pág. 533

[2] CARNELUTTI citado por LARRAUD (Rufino), Curso de Derecho Notarial, Editorial Depalma, Buenos Aires, p. 197.

[3] Código Procesal Civil, Sétima Edición, San José. Editorial Investigaciones Jurídicas, S.A. 1.999, artículo 368.

Como lo indica la definición general citada supra, para el ámbito del Derecho, los documentos deben servir de prueba. Es a ello que atribuimos que nuestro Código Procesal Civil recoja una concepción tan amplia de documento como toda cosa mueble que sirve de prueba, pretendiendo no quedarse rezagado en relación con los avances tecnológicos y su incorporación a los procesos como medios de prueba. Esta concepción tan amplia no hay que perderla de vista, para el desarrollo de nuestro tema, en cuanto a los documentos realizados por medios electrónicos.

El documento público notarial aparece como un medio para que las partes declaren su voluntad y sirvan para comprobar dicha declaración; surge como consecuencia de una necesidad social para regular el tráfico jurídico, pues le otorga validez probatoria a los actos, declaraciones y contratos.

El documento público notarial está referido a la persona que los autoriza y de su capacidad para dar fe pública notarial, de los actos o contratos que se realicen en su presencia. Este documento tiene su fundamento en su fuerza probatoria, que se deriva de la fe pública del Notario que lo expide con arreglo a la ley.[1]

---

[1] PALLARES (Eduardo) Diccionario de Derecho Procesal Civil. México. Editorial Porrúa S.A. Edición décimo sexta. 1.984, pág. 291.

Existen diversas definiciones de documento público notarial, las cuales atienden a la persona que los emite, al documento en sí, al contenido del mismo o al cumplimiento de requisitos para su constitución. Así Giménez Arnau aludiendo al contenido expone que "es el documento público autorizado por Notario, producido para probar hechos, solemnizar o dar forma a actos o negocios jurídicos y asegurar la eficacia de sus efectos jurídicos."[1]

El documento notarial es el instrumento público por excelencia. Se presume que todo documento expedido o autorizado por un notario público se reputa notarial, inclusive nuestro Código Notarial establece como instrumento notarial los documentos en los que interviene un agente consular en su función notarial.

Siendo que los documentos notariales son los emitidos por el Notario Público es importante saber quiénes tienen esta investidura.

Nuestro Código Notarial define al Notario Público como "el profesional en Derecho, especialista en Derecho Notarial y Registral, habilitado legalmente para ejercer la función notarial. En leyes, reglamentos, acuerdos y documentos, cuando se use la palabra notario debe entenderse referida al notario público."[2]

---

[1] GIMÉNEZ ARNAU (Enrique) Derecho Notarial. Pamplona. Ediciones Universidad de Navarra, Segunda Edición, 1976, pág. 412.

[2] Código Notarial. Ley 7774 del 22 de mayo de 1.998. San José, Editorial Investigaciones Jurídicas S.A., Primera Edición, Edición concordada por el Lic. Herman Mora, julio del 2.000, art. 2.

De la misma manera, en cuanto a la función notarial de los Cónsules, el Código Notarial establece que se les autoriza a ejercer el Notariado Público en su circunscripción territorial, respecto de los hechos o contratos que deben ejecutarse o surtir efectos en Costa Rica y realizarla de conformidad con lo establecido en dicho Código.[1]

a) Elementos del documento

En todo documento concurren tres elementos: corporalidad, autor y contenido. En el notarial debe además agregarse las solemnidades prescritas por la ley.

i- Corporalidad:

La corporalidad o expresión (grafía) se refiere "a la pieza material que lo contiene o soporte físico que lo integra y forma parte de él"[2]. Estos documentos necesitan para su existencia un soporte material, directamente relacionado con el hecho de que el documento notarial debe cumplir con su función de ser prueba preconstituida. En el desarrollo de esta investigación analizaremos el tema de la corporalidad del documento notarial desde al óptica informática.

ii- Contenido:

---

[1] Ibid, artículo 14

[2] PELOSI (Carlos). El documento notarial. Buenos Aires. Editorial Astrea de Alfredo y Ricardo de Palma. 1992. pág. 125.

El contenido por su parte, es aquello que el Notario percibe. Es el hecho histórico relatado por él o la declaración de otra persona. El Notario capta los hechos y los archiva en su memoria ordenadamente, sin ser actor de los hechos que se propone describir en el documento. Los hechos relatados no pueden ser alterados, ya que por medio de la firma de los otorgantes estos dan su asentimiento a lo descrito en el documento notarial. [1]

iii- Formalidades:

Las formalidades se refieren a los presupuestos formales que establece la ley para cada acto.

El Código Notarial dice que "los documentos notariales deben estar manuscritos o mecanografiados, caracteres legibles y tinta o impresión indelebles . El texto del documento debe escribirse en forma continua, sin dejar espacios en blanco. Siempre deberán respetarse los márgenes, pero carecerán de validez las palabras escritas fuera de ellos, salvo que se trate de notas marginales en el protocolo, autorizadas por la ley. Excepto las escrituras matrices del protocolo, los documentos que el notario autorice deben llevar siempre su firma, el sello blanco, el respectivo código de barras y cualquier otro medio idóneo de seguridad, determinado por la Dirección Nacional de Notariado. Los documentos inscribibles

[1] PELOSI Carlos. Op.cit., pág. 124.

en el Registro Nacional, además de los requisitos anteriores, deben cumplir con los requisitos de seguridad establecidos por esta institución."[1]

iv- Sujeto:

El autor es el Notario quien se encuentra revestido de cualidades y condiciones necesarias que lo legitiman en su actuación. Según nuestro ordenamiento los Notarios Públicos son los únicos autorizados para realizar la función notarial. La legitimación del Notario se encuentra directamente relacionada al tema de la fe pública, ya que es realmente este instituto el que legitima las acciones realizadas por el Notario.[2]

b) Clasificación de los documentos notariales:

Los documentos notariales se pueden clasificar en diferentes tipos dependiendo de su contenido, eficacia, efectos, forma instrumental, colección o guarda, etc. Si se estudia profundamente estos tipos se podrían desarrollar otras subdivisiones.

El autor Carlos Pelosi hace la siguiente clasificación de los documentos notariales: a) Originales o reproducciones, atendiendo a la genuinidad de los documentos; b) Protocolares y extraprotocolares, si el documento forma parte por cualquier medio posible de un protocolo notarial.[3]

---

[1] Código Notarial, artículo 73.
[2] Código Notarial, artículo 1
[3] Pelosi, Carlos, Op.cit. página 243

Enrique Giménez Arnau, por su parte, clasifica los documentos notariales de la siguiente manera: a) Protocolares, en el que incluye a las escrituras públicas, las actas y los documentos protocolados (judiciales o privados); b) Extraprotocolares, donde se incluyen los testimonios de legitimidad de firmas y legalizaciones, certificados de existencia y de vigencia. [1]

Como expusimos existen varios criterios para clasificar los documentos notariales. Para el desarrollo de nuestra investigación analizaremos la clasificación de los autores mencionados, que coinciden con el criterio de clasificación que realiza nuestra ley notarial, que distingue dos clases de documentos notariales:

a) Los documentos notariales protocolares y
b) Los documentos notariales extraprotocolares, siguiendo el criterio de que su original se extienda en el Protocolo Notarial o fuera de el.[2]

i- Documento notarial protocolar:

Para nuestro Código Notarial, al igual que para los autores mencionados, son documentos notariales protocolares los que se extienden en el Protocolo Notarial.

[1] Giménez Arnau, Enrique. Op.cit. página 406
[2] Código Notarial,, artículo 80

Son documentos cuya matriz cumple con todas las características necesarias para ser un documento notarial.

Como hemos dicho, de esta clasificación de documentos notariales protocolares, se pueden hacer a su vez otras subdivisiones. Nuestro Código, siguiendo la doctrina, establece que son documentos notariales protocolares las escrituras públicas, las actas notariales y las protocolizaciones consignadas en el protocolo del notario.[1]

Las escrituras públicas son, por naturaleza propia, el documento notarial protocolar sin discusión. El Notario debe confeccionarlas con las formalidades que la ley impone y apegarse a la manifestación de la voluntad de las partes comparecientes, conforme lo establece el artículo 81 del Código Notarial.

"La escritura pública es aquel instrumento público donde se plasma una declaración de voluntad, con el propósito de producir algunos efectos jurídicos, es decir, un negocio jurídico. En ella se manifiesta y perpetúa, como prueba documentaria, la formalización de un acto o contrato. Siendo así es que la escritura usualmente va referida a la creación, modificación, extinción o cancelación de una relación jurídica. Esa manifestación de voluntad puede ser

[1] Código Notarial, artículo 80.

unilateral (testamento), bilateral (una venta), o multilateral (constitución de una sociedad).[1]

En la escritura pública se da el principio de la unidad del acto, pues hay identidad de la actuación, las personas, el tiempo y el espacio. Un punto interesante de nuestra investigación es la superación o nueva conceptualización de este principio, en razón de la aplicación de las nuevas tecnologías en la producción de documentos en que se da la expresión de voluntad de las partes.

Las Actas Notariales son un segundo tipo de documento notarial protocolar, a la cual se le aplican, en lo pertinente, las disposiciones de las escrituras públicas, con las salvedades hechas por ley. Es un instrumento público en el cual el Notario mediante la fe pública autentica o hace constar hechos, sucesos, situaciones, notificaciones, prevenciones o intimaciones que procedan según la ley. [2]

En las Actas Notariales no es necesaria la comparecencia de partes, ni su firma, sino únicamente la constancia del acto, salvo que legalmente sea necesario o se trate de un perito. También se puede romper el principio de la unidad del acto y del tiempo, pues el hecho no es algo fijo, sino que el Notario narra lo que esta

---

[1] Mora Vargas, HERMAN. Manual de Derecho Notarial: La Función Notarial, Editorial Investigaciones Jurídicas S.A., Primera Edición, San José, 1999, página 213.
[2] Código Notarial, artículo 101.

ocurriendo en el transcurso del tiempo en que esta realizando el acta o posteriormente, siempre que sea dentro de las siguientes veinticuatro horas.[1]

Las Actas se pueden clasificar dependiendo de su finalidad y de lo que se quiera hacer constar. Por ello existen actas de presencia, de referencia, de notoriedad, de notificación, de requerimiento y de depósito.[2]

Las Protocolizaciones son la transcripción de documentos privados o piezas judiciales en el Protocolo. Esta transcripción puede ser literal, en lo conducente o en referencia, lo cual se debe indicar en la protocolización, lo que se realizará dependiendo de los fines jurídicos que se pretendan El Notario debe guardar copia del documento privado en su Protocolo de referencias, para comprobar su existencia y los detalles de su contenido.[3]

Cuando se protocoliza un documento privado, aunque se le aplican los requisitos formales de las escrituras públicas, dicha protocolización no adquiere el efecto de estas en sentido estricto.[4] Dentro de los efectos no se encuentra lograr inscripciones en los registros ni oficinas públicas, con las excepciones prescritas por ley.

---

[1] Código Notarial, artículo 102.
[2] Mora Vargas, HERMAN, Op. Cit,. Páginas 226-228 y Pelosi, CARLOS, Op. Cit. Página 55
[3] Código Notarial, artículos 47, 105 y 110.
[4] Mora Vargas, HERMAN, Op.cit. p. 230

Las protocolizaciones tampoco constituyen plena prueba en un proceso judicial o administrativo, sino solamente sirven como prueba indiciaria, ya que puede ser necesaria la presentación del documento original para fundamentar el derecho real que se pretenda.[1]

ii- Documento Notarial extraprotocolar:

Nuestra legislación notarial los define como los documentos en que conste cualquier actuación o diligencia que el Notario, autorizado por ley, lleve a cabo fuera del Protocolo.[2]

Son los documentos Notariales cuyos originales se extienden fuera del Protocolo Notarial, se extienden en original y están destinados a circular cuando se le entrega al interesado.

Estos documentos los expide el Notario con las formalidades de la ley, en el ejercicio de sus funciones y dentro de los límites de su competencia. Habrá tantos documentos fuera del Protocolo con fe originaria, en razón al principio de inmediación autorizado por las normas que rigen la materia.[3] En estos documentos se pone a plena prueba la fe pública notarial reconocida por ley.

---

[1] Código Notarial, artículo 10
[2] Ibid, Artículo 108.
[3] Pelosi, Carlos, Op.Cit., página 249

El elemento sobresaliente y definitorio de estos documentos notariales, es su independencia del Protocolo; y esa particularidad de independencia hace que pueda ocurrir: a) que existan tantos originales como partes interesadas, b) el Notario conserve un ejemplar, y c) que, a pedido de los intervinientes, una vez producido el documento sin matriz, se pueda incorporar al Protocolo mediante un Acta o Protocolización.[1]

Al igual que en los documentos protocolares, la clasificación de documentos extraprotocolares admite una subdivisión generalmente aceptada en las legislaciones que siguen el Sistema de Notariado Latino y la doctrina en que se sustentan.

Nuestra legislación clasifica e incluye dentro de dichos documentos extraprotocolares, las reproducciones de instrumentos públicos, certificaciones de documentos, piezas de expedientes o inscripciones, traducciones, actas, diligencias y otras actuaciones que el Notario Público, autorizado por ley, extiende fuera del protocolo.[2]

El Código califica las reproducciones de los instrumentos públicos, como un documento extraprotocolar, por ser un documento accesorio del que se encuentra

[1] PELOSI Carlos. Op.cit., página 250.
[2] Código Notarial, artículo 108

en el Protocolo y pueden consistir en testimonios, certificaciones y copias auténticas.[1]

Los Notarios dentro de su labor extraprotocolar y bajo su responsabilidad, pueden extender certificaciones relativas a inscripciones, expedientes, resoluciones o documentos existentes en Registros y oficinas públicas. También pueden certificar documentos privados, en cuyo caso deben dejarse copia auténtica. [2]

En estos documentos deben cancelarse las especies fiscales, los timbres y derechos que deban cubrirse según el arancel existente y tendrán el valor que la ley les conceda mientras no se compruebe que carecen de exactitud.

El Notario también puede autorizar traducciones de documentos redactados en idioma distinto del español, debiendo adjuntar a su traducción, el documento traducido o su copia auténtica.[3]

Todos estos documentos notariales extraprotocolares tienen la peculiaridad de que si se presentan para hacer valer derechos en un proceso judicial o administrativo y su autenticidad es cuestionada, se deberá presentar el documento original.[4]

---

[1] Código Notarial, Artículo 112.
[2] Ibid,, artículo 110.
[3] Ibid, artículo 109.
[4] Ibid, artículo 107.

c) Fines del Documento Notarial

La doctrina establece determinados fines al documento notarial. El Licenciado Herman Mora Vargas, reconoce dentro de los fines tres funciones primordiales: "a) dar forma a hechos y voluntades, b) con la forma los constituye sustantivamente, y c) se presentan como prueba privilegiada."[1]

Dichos fines son consecuencia directa de la función notarial, que al crear un instrumento público genera de forma inmediata esos fines. Ese instrumento público creado por el Notario se vincula estrechamente a la forma, a la prueba y al negocio jurídico que contiene, al mismo tiempo tendrán efectos sustantivos, civiles, procesales y ejecutivos del documento.

La finalidad originaria del documento notarial ha sido su evidente propósito probatorio. Conforme el Derecho Notarial evoluciona, ha demostrado que en la actualidad el documento notarial cumple, además con otros fines, a saber:

i- Dar forma a hechos y voluntades:

El documento notarial refleja la manifestación final de la voluntad de los comparecientes o de hechos que pretenden formalizarse.

"La forma de los documentos notariales tiene que existir porque es la

---

[1] MORA VARGAS, (Herman), Op.cit,. pág. 193

exteriorización de las voluntades jurídicas vinculantes. Para que el exterior conozca esta declaración de voluntad generada en su interior y adquiera valor ante todo el mundo, hay que darle forma. Hay que mostrar la realidad que se revela, volcarla en un molde que preparará el hombre perito en derecho y dador de autenticidad, al que llamamos escribano, o funcionario autorizante, y entonces la o las relaciones jurídicas, nacen a la vida en forma de escritura pública."[1]

La forma en la disciplina jurídica es importante, precisamente, la forma hace que los documentos notariales sean diferentes a otros tipos de documentos, y ayuda a su vez a sistematizar el derecho notarial poniendo de esta forma en movimiento dicha función.

Al pasar de los años, los documentos notariales se han caracterizado por su forma, dándole a los negocios mayor seriedad y un carácter de "obligatoriedad", por decirlo de algún modo, a lo descrito en él. Las partes al firmar el documento conocen por lo menos de una forma interna, que lo manifestado puede tener consecuencias jurídicas importantes.

"En una palabra, van a dar forma legal al contrato verbal que celebraron cuando después de discutir las condiciones y el precio, se dieron quizá la mano

---

[1] GONZALEZ (Carlos E.) Derecho Notarial. La Ley Sociedad Anónima Editora e Impresora, Buenos Aires, Argentina, 1.971. pág. 202.

(reminiscencia de la antigua "Palmata") y el trato quedó hecho. Esto es el progreso del derecho contemporáneo; antes quedaba finiquitado así el convenio y ahora se complementa con la presencia del depositario de la fe pública y la ejecución de diversos requisitos de forma."[1]

Podríamos afirmar que la forma es el verdadero fin, constituir el negocio jurídico, hacer existir, dar vida, configurar, estructurar jurídicamente.

Hasta este punto consideramos que la función más importante del documento notarial es darle forma a determinado negocio, es más, se podría afirmar que el documento notarial nace con el fin de configurar un negocio jurídico para posteriormente, en caso de ser necesario, se tenga que probar dicho negocio. Con esto queremos decir que el documento notarial no se realiza necesaria y solamente para constituir medio de prueba - ya que esa función se daría con posterioridad a un hecho contencioso - sino para formalizar un negocio entre partes o una manifestación de voluntad unilateral.

No puede negarse que el documento notarial es la prueba más eficaz, sin más impugnación que la declaratoria de falsedad, pero esta finalidad puede que se de y puede que no sea necesaria por una conclusión satisfactoria del negocio formalizado.

---

[1] GONZALEZ, (Carlos E.) Op.cii., 314.

ii- Servir de prueba preconstituida:

Tal es el valor que se le da a los documentos notariales que nuestro ordenamiento lo hace plenamente. El Código Procesal Civil otorga valor probatorio a los documentos o instrumentos públicos, mientras no sean argüidos de falsos, hacen plena prueba de la existencia material de los hechos que el oficial público afirme en ellos haber realizado o haber pasado en su presencia, en el ejercicio de sus funciones.[1]

El cuerpo de leyes citado supra, establece que dicho documento no solo da fe de la existencia de la convención o disposición para la prueba, sino aún de los hechos o actos jurídicos anteriores que se relatan en él, en los términos simplemente enunciativos, con tal de que la enunciación se enlace directamente con la convención o disposición principal. Las enunciaciones extrañas a la convención o disposición principal, no podrán servir para otra cosa que no sea la del principio de prueba por escrito.[2]

Referirse a prueba preconstituida quiere decir que es prueba preparada con anterioridad a una contención futura; prueba escrita que está en ese instrumento y que si alguna vez la necesitamos, la presentaremos de inmediato para hacer valer

---

[1] Código Procesal Civil, artículo 370.
[2] Ibid, artículo 371.

nuestros derechos. Cuando se estudia el documento notarial como prueba preconstituida es necesario referirse al derecho procesal, que será auxiliar en esta tarea. Debe quedar claro que el documento notarial siempre servirá para formalizar una relación, pero no siempre será necesario usarlo como prueba ya que muchos instrumentos de actos jurídicos no llegan a ser empleados como prueba preconstituida.

Dicha prueba se forma con anterioridad al proceso por precaución, sin saber si en el futuro se presentará un litigio que haga necesario su utilización. Para que la prueba sea preconstituida no basta que se haya formado con anterioridad al proceso, sino que exista la intención de darle al documento notarial ese fin, "por ello no son tales, los documentos que fueron creados sin preveer la iniciación de un litigio."[1]

iii- Eficacia

Es importante tomar en cuenta que la eficacia es también una de las funciones del documento notarial.

"Por otra parte, no basta que un acto se produzca externamente con arreglos a las formas adecuadas, ni basta que sea auténtico para que el derecho sea eficaz; la

[1] MARTINEZ NAVARRETE (Doroteo) El Documento Público Notarial, Tesis para optar al grado de Licenciatura en Derecho, Facultad de Derecho .Universidad de Costa Rica, 1980, Pág. 37.

eficacia se consigue, con la presunción de validez que se deriva de la calificación notarial."[1]

Como hemos analizado, el documento público notarial tiene como fines el de ser un medio de prueba y un medio para constituir o extinguir relaciones jurídicas, dándoles legitimidad, certeza y publicidad. "Esas funciones son más que manifestaciones de la eficacia que en las diversas esferas y relaciones de la vida el documento público notarial produce."[2]

Nuestro Código Notarial establece los efectos de los instrumentos públicos en el artículo 24, que dice: " *La existencia del instrumento público se comprueba mediante el original o las reproducciones de la matriz legalmente expedida. Produce, por sí mismo, los efectos jurídicos que deban derivarse de la voluntad de los otorgantes; obliga a las oficinas correspondientes para darle el trámite necesario a fin de cumplir lo querido por los otorgantes y prueba, también por sí mismo, los hechos, las situaciones y las demás circunstancias de que el notario haya dado fe en el ejercicio de su función.*"[3]

---

[1] MARTINEZ NAVARRETE (Doroteo). Op.cit., pág. 45.
[2] Ibid , pág. 47. citando a Rodríguez Arnau.
[3] Código Notarial, artículo. 124.

Sección II: FE PUBLICA NOTARIAL

a) La fe en sentido amplio.

Para iniciar el tema de la fe pública notarial es importante conceptualizar lo que es fe y además lo que significa la fe pública en general, ya que no sólo los Notarios gozan de ella.

Entre algunos de los conceptos que se conocen de fe tenemos el aportado por Rufino Larraud, "La palabra *fe* puede utilizarse con distintos significados. Fe es la creencia o confianza en algo que no hemos percibido por nuestros propios sentidos, y que aceptamos por la autoridad de quien lo dice, o por la fama pública; también es fe la seguridad que se da, o la afirmación que se hace, acerca de la verdad de algo; y desde otro punto de vista, la fe es una cualidad: un grado de eficacia demostrativa que algo tiene."[1]

Este concepto se encuentra estrechamente ligado a la idea de *verdad.*

¿Qué es fe? Creencia o convicción, persuasión, certeza, seguridad, confianza en la verdad de algo que no se ha visto por la honradez o autoridad que se reconoce a la persona que da testimonio de ello.

---

[1] LARRAUD (Rufino), Curso de Derecho Notarial, Editorial Depalma, Buenos Aires, 1976.pág. 636.

b) La Fe Pública

Con base en lo anterior podemos afirmar, que la fe pública es la potestad de infundir certeza a actuaciones, hechos y actos jurídicos, impregnándolos de una presunción de verdad por medio de la autenticidad conferida a los documentos que los prueban.

Clases de fe pública:

La fe pública supone una verdad y presume creencia. Esto es así por seguridad, armonía y estabilidad. Se puede encontrar cuatro tipos de fe pública según la clasificación que hace Enrique Giménez Arnau:

"a) Fe pública administrativa: Su objeto es dar notoriedad y valor de hechos auténticos a los actos realizados por el Estado o por las personas de Derecho Público dotadas de soberanía, de autonomía o de jurisdicción. El contenido de la fe pública administrativa comprende no sólo los actos pertenecientes a la actividad legislativa o reglamentaria, sino también a los actos jurisdiccionales, a los de mera gestión. Esta fe pública administrativa se ejerce a través de documentos expedidos por las propias autoridades que ejercen la gestión administrativa en los que se consignan órdenes, comunicaciones y resoluciones

de la Administración.

b) La fe pública judicial: Las facultades o limitaciones establecidas en la norma objetiva, pueden dar lugar a contienda o pugna entre el Estado y los particulares, o entre dos particulares. Dada la trascendencia de las actuaciones ante los Tribunales civiles, administrativos o contencioso-administrativos lógico que todas estas actuaciones estén revestidas de un sello de autenticidad que se imprime en ellas en virtud de la fe pública judicial.

c) La fe pública extrajudicial o fe pública notarial: Hay un incontable número de actos humanos cuya finalidad es la constitución, modificación o extinción de relaciones jurídicas y por ende de derechos patrimoniales de carácter privado. La constatación de semejantes acontecimientos constituye la órbita propia de la fe pública notarial.

d) La fe pública registral: Todavía había que establecerse una nueva categoría si se acepta la posición de Lavandera, que considera el Registro Inmobiliario como una manifestación de la fe popular. "[1]

Otra de las clasificaciones de fe pública la elabora el autor Carlos E. González estableciendo las siguientes: Notarial: cuando el depositario de esa fe

[1] JIMÉNEZ ARNAU (Enrique) Op.cit., pág. 44.

es el escribano; Judicial: cuando es el actuario de juzgados y Administrativa: ejercida por ciertos funcionarios públicos que forman parte de la Administración Pública del Estado.[1]

La expresión *fe pública* no es más que una especificación adjetiva del sustantivo *fe*, y, por tanto, tiene muy diversos sentidos que corresponden a la acepción que cada uno tenga de lo que es la *fe*.

La fe pública ha sido relacionada directamente con el concepto de función notarial, ya que se le atribuye al Notario Público dicha dación de fe. El autor Carlos.E. González indica que "La más antigua y clásica doctrina sobre la función notarial, afirma González Palomino, es la que centra en el concepto de fe pública: La función del notario es la de dar fe de ciertos actos; y el valor del instrumento el de hacer fe de su existencia y de todo o parte de su contenido."[2]

Como parte de la función notarial, está la fase autenticadora en la que el Notario imparte fe pública a los hechos o actos jurídicos ocurridos en su presencia. La fe pública notarial es una especie del género "fe pública" y ésta a su vez es una especie de la "fe".

---

[1] GONZALEZ (Carlos E.) Op.cit., pág. 209.
[2] Ibid, pág. 204.

"La fe pública, es el poder que compete al funcionario para dar vida a las relaciones jurídicas, constituyendo una garantía de autenticidad. La da el Estado a determinados individuos mediante ciertas condiciones que la ley establece, destacándose especialmente la notarial, por los requisitos de gran honorabilidad, título habilitante especial e incompatibilidades (dedicación exclusiva a la función fedataria) impuestos a los que con ella son investidos."[1]

Nos parece que del concepto anterior deriva la fe pública notarial, siendo los Notarios Públicos solamente un sector de funcionarios que la poseen.

En síntesis, no puede existir instrumento público sin fe pública, pues es en este donde se manifiesta, incluyéndose dentro de los instrumentos públicos los documentos notariales protocolares y extraprotocolares.

c) Fe Pública Notarial:

Según González Palomino "la fe pública notarial consiste en la certeza y eficacia que da el poder público a los actos y contratos privados por medio de la autenticación de los notarios" y dice bien, puesto que la fe pública es principalmente certeza, asentimiento, verdad que se presta a la manifestación del

---

[1] GONZALEZ (Carlos E.) Op.cit., pág. 208.

funcionario, autoridad legítima que a éste se atribuye para que las escrituras por él autorizadas sean auténticas y sus respectivos contenidos tenidos por ciertos."[1]

La consecuencia directa de la fe pública notarial es la autenticidad (uno de los fines del documento público notarial); esta fe da presunción de verdad, garantiza el cumplimiento de los convenios, dándole a los instrumentos notariales firmeza, irrevocabilidad y ejecutoriedad. Hace que el instrumento valga por sí mismo.

La fe pública es al notariado, lo que la jurisdicción -en sentido estricto- es al juez: una atribución de poderes determinados.[2]

Lo que diferencia la fe pública notarial de su género (fe pública) está en que la notarial se refiere a actos privados exclusivamente extrajudiciales.

Si la actuación del Notario no tuviera una finalidad fundamentalmente probatoria, si el instrumento notarial no probara nada, no se podría hablar de fe pública notarial.

---

[1] GONZALEZ (Carlos E.) Op.cit., pág. 209.
[2] LARRAUD (Rufino) Op.cit., página 645.

CAPITULO II:

ACTUACIONES NOTARIALES FORMADAS EN EL EXTRANJERO

Sección I: LA ACTIVIDAD CONSULAR

La institución consular como legación permanente, apareció en el Siglo XIII cuando Venecia, Pisa y Génova, ciudades del Norte de Italia, establecieron la práctica de mantener entre sí, representantes en dichas ciudades. Los primeros cónsules tenían como función el arreglo de cuestiones exteriores. Posteriormente en el Siglo XIV los italianos nombraron cónsules en los Países Bajos, Alemania, España, Francia y Gran Bretaña.[1]

Durante la Edad Media se crearon Cónsules permanentes, en razón del acrecentamiento del poder estatal. En un principio los Cónsules fueron los únicos agentes permanentes que tenían los Estados en el extranjero, ocupándose además de los intereses políticos. [2]

Conforme se fue imponiendo y fortaleciendo la costumbre de establecer relaciones económicas, comerciales, aéreas y marítimas entre los Estados, se da la necesidad de instaurar representaciones diplomáticas. Paralelo a este evento, se da en los Estados la división en la función exterior entre lo político y lo comercial.

---

[1] CAMARGO (Pedro Pablo) Tratado de Derecho Internacional, tomado de la Antología de Lecturas de Derecho Internacional Público I, Facultad de Derecho, Universidad de Costa Rica, 1998, p.412.
2 CRUZ CIENFUEGOS (Jorge Ernesto) La Función Notarial en el Servicio Exterior, su regulación en los países centroamericanos y particularmente en el Derecho salvadoreño y costarricense, Facultad de Derecho, Universidad de Costa Rica, 1979, p.27.

Con el desarrollo de las representaciones diplomáticas, la institución consular decayó hasta reducirse a proteger los intereses comerciales y de navegación de los nacionales del país que representaban.

Cuando se da esta división en la función exterior de los Estados, se dio la necesidad de reglar y establecer rangos entre los agentes diplomáticos, siendo así como renace la institución consular. [1]

Conforme se fue extendiendo las relaciones jurídicas entre ciudadanos de diferentes nacionalidades o que se encuentran viviendo en dos o más Estados, fue resultando la necesidad de tener y nombrar personas que representaran a sus nacionales en el extranjero. Estas personas los Estados les enviste de ciertas facultades, para darle validez y eficacia a los contratos y actos jurídicos que debían ser cumplidos o consumados en una nación y formalizados o exteriorizados en otros.

En razón de la necesidad de tener una persona autorizada para dar validez a actos y contratos de nacionales en el extranjero o de actos y contratos de ciudadanos extranjeros que deben tener eficacia en otro Estado y ante la falta de

[1] CAMARGO (Pedro Pablo) Op. Cit., p. 427

funcionarios pertenecientes a la carrera notarial para ello, se conceden facultades notariales a los Agentes Diplomáticos o Jefes de Misión y a los Cónsules. [1]

a) Fundamento de la Actuación Notarial.

La actuación Notarial de los Cónsules tiene su fundamento en una regla denominada: "LOCUS REGIT ACTUM", que es un "principio de Derecho Internacional Privado, según el cual le ley territorial rige la forma de los actos jurídicos."[2]

Esta regla es contraria al principio que comúnmente se utiliza que es la "LEX FORI", la cual indica que el acto debe sujetarse a la ley del lugar donde se lleve a cabo.

En un principio para la aplicación de la norma lex locus actum se recurrió a la ficción de la extraterritorialidad, que equipara la Sede Consular al territorio nacional; por lo que todo acto realizado en dicha Sede aplicando los requisitos y la forma vigentes en su país, sería autentico y válido por estar realizado ficticiamente en territorio nacional.

Aunque la locus regit actum nació como una excepción al no sometimiento a

---

[1] CRUZ CIENFUEGOS, Jorge Ernesto, Op.cit., p. 22
[2] PALLARES, Op.cit. página 554

las formas válidas del lugar donde se realiza el acto jurídico; actualmente se establece como una norma imperativa en cuanto a su aplicabilidad, cuando la ley territorial donde se ejecutará el acto es diferente al lugar donde se realiza, y cuando el funcionario que interviene aplica la ley de su país.[1]

En este sentido se puede decir que los actos consulares implican una limitación a la aplicación del efecto territorial de las leyes del Estado receptor. Esto por cuanto dichos actos, son de derecho interno realizados en el extranjero.

La función notarial de los Cónsules es muy importante por cuanto al no existir una uniformidad internacional en las escrituras públicas, se abre la posibilidad a los nacionales y extranjeros de realizar actos válidos en un país, que tendrán su eficacia en el país donde ellos quieren que sus actos tengan efecto.

Para que dicha actuación Notarial tenga validez, es común que requieran de una legalización que se realiza en el Ministerio de Relaciones Exteriores. Esta legalización no influye en la autenticidad de la escritura, sino que establece que el funcionario que la realizó esta debidamente autorizado para ello, previniendo con ello cualquier posibilidad de fraude.

---

[1] JIMÉNEZ-ARNAU (Enrique) Op.cit., página 381-382

b) Marco regulador de dicha actividad.

La institución consular se desenvuelve consuetudinariamente y tiene su primera codificación multilateral con la Convención de Viena sobre Relaciones Consulares # 3767 de 1963. Esta normativa tuvo su razón de ser y llevo a garantizar el mejor desempeño de las funciones del Cónsul.

Las funciones del Cónsul están reguladas por el Código de Derecho internacional Privado o Código Bustamante y la Ley Orgánica del Servicio Consular, que contiene normas en donde se da primacía a las normas del Estado que envía ante las normas del Estado receptor, sobre todo en caso de que no hayan entre ellos una oposición clara y manifiesta, pues cuando hay oposición se debe recurrir a las normas y principios del Derecho Internacional Privado.[1]

En el desempeño de su cargo el Cónsul debe cumplir lo dispuesto por los tratados, leyes y reglamentos del país que representan y del Estado ante el cual se encuentran acreditados.

Entre la funciones que la legislación consular, tanto internacional como nacional, le atribuyen a los agentes consulares están las de tipo notarial. Esta y la

[1] HERRERA DURAN (RITA) y VILLALOBOS SOTO (JOAQUIN) Derecho Consular Costarricense. Tesis para optar al título de Licenciados en derecho Facultad de Derecho. Universidad de Costa Rica, 1983 ,p.165.

actuación como funcionario del Registro Civil, figuran entre la funciones consulares clásicas.

Aunque desde el siglo pasado se extendió el campo de actuación de los Cónsules a los actos notariales, es la Convención de Viena en la Sección sobre el establecimiento y ejercicio de las relaciones consulares, que dispone como una de las funciones consulares la de "actuar en calidad de notario, en la de funcionario del Registro Civil y en funciones similares y ejercitar otras de carácter administrativo, siempre que no se opongan las leyes y reglamentos el Estado receptor."[1]

La Ley Orgánica del Servicio Consular siguiendo la normativa internacional, establece que "Los funcionarios consulares son agentes comerciales, administrativos, notariales y encargados del Registro Civil de la República."[2]

En Costa Rica los Cónsules son funcionarios nombrados por el Poder Ejecutivo por intermedio del Ministerio de Relaciones Exteriores, por lo que sus nombramientos, independientemente de ejercerlo con la mayor idoneidad, son por un máximo de cuatro años, en razón al cambio de Administración.

---

[1] Convención de Viena Sobre Relaciones Consulares, Ley #3767 del 3 de Noviembre de 1966, artículo 5, inciso f).
[2] Ley Orgánica del Servicio Consular, #46 del 7 de Junio de 1925, Artículo 13.

Aunque se puede interpretar que los Cónsules son auxiliares de la misión diplomática y tienen cierta subordinación a ella, tienen total independencia en las funciones legales, notariales y de Registro Civil.

La Ley Orgánica del Servicio Consular, en cuanto a la actuación de los Cónsules como Notarios Públicos, desarrolla un capítulo especial que denomina " De la Fe Pública de los Cónsules". Dicho capítulo tiene singular importancia para este estudio, por cuanto en sus artículos se reviste a los Cónsules de la República, el carácter de Notarios, otorgándoles autoridad para dar fe, siempre sujeta a las leyes, actos y contratos.[1]

Los nacionales y extranjeros pueden comparecer ante el Cónsul de Costa Rica, nombrado en alguna ciudad del país que se encuentre, a otorgar documentos públicos que tengan sus efectos y se ejecuten en Costa Rica.

El Código Notarial establece que el Cónsul ejercerá el notariado público en su circunscripción territorial "respecto de los hechos, actos o contratos que deben ejecutarse o surtir efecto en Costa Rica". [2]

Los Cónsules en su función notarial deben llevar un Protocolo con las escrituras matrices otorgadas y autorizadas, de la misma forma en que los notarios

---

[1] Ley Orgánica del Servicio Consular, artículo 56.
[2] Código Notarial, artículo 14.

públicos llevan su protocolo notarial. Cuando el Cónsul deja el cargo, se produce de pleno derecho su cesación en la función notarial, por lo que debe devolver del protocolo en el estado que está con su respectiva razón de cierre.[1]

La Convención de Viena no hace ninguna distinción, del tipo de oficina consular requerida para ejercer el notariado, pues recordemos que esta el Cónsul General, Cónsul, el Vicecónsul o la Agencia Consular.

La Dirección Nacional de Notariado, puso en conocimiento una directriz dirigida al cuerpo consular, que establece que el protocolo es un instrumento de uso personalísimo por parte del funcionario consular. Recomienda que el protocolo lo utilice el Cónsul General y que no es admisible que aparezcan autorizando escrituras otras personas distintas de quien se le autorizo, por lo que emite directriz para insertar una razón y continuar el uso dl protocolo conforme al Código Notarial.[2]

Los instrumentos otorgados ante los Cónsules, surten los mismo efectos que los otorgados ante Notario Público, siempre que observen las formalidades que las leyes impongan para su validez.[3]

---

[1] Código Notarial, artículo 14.
[2] Directriz #003-98, de la Dirección Nacional de Notariado, de las 10 horas 30 minutos del 24 de noviembre e 1998.
[3] Ley Orgánica del Servicio Consular, artículo 68.

Cuando el Cónsul cese en sus funciones, el Ministerio de Relaciones Exteriores y Culto debe comunicarlo a la Dirección Nacional de Notariado, pues como se dijo antes, mientras el Cónsul se encuentre en funciones será notario Público por ministerio de Ley por lo que debe cumplir las mismas obligaciones de los Notarios Públicos nacionales.

SECCION II: Actuación notarial extraterritorial.

Cuando se requiere realizar actos cuya eficacia se dará en Costa Rica, comúnmente se recurre al Cónsul en su función notarial, por lo que no es frecuente encontrar Notarios Públicos autorizando escrituras cuando se encuentran fuera de su patria.

La regla general en casi todos los países, es que los Notarios pierdan su competencia fuera de su nación. Inclusive hay legislaciones en que el Notario solamente puede ejercer su funcion en determinada área geográfica o circunscripción dentro del mismo territorio nacional.

Esta norma se aplica aún en paises que siguen el Sistema Notarial Latino, como por ejemplo, en la República Federal de México existe una Ley de Notariado exclusiva para el Distrito Federal, en la que se regla todo lo referente al ejercicio de la función notarial aplicable solo a la capital mexicana y no al resto de la República.

En países como México con una enorme extensión territorial, se justifica la limitación a la competencia en razón de territorio, del ejercicio de la función notarial. Las justificaciones a dicha limitación no son aplicables a nuestro país ni al resto de países centroamericanos, exceptuando a Panamá y Belice.

a) Normativa que rige la actividad notarial extraterritorial.

El fundamento de la legalidad de esta actuación se encuentra en la misma regla de Derecho Internacional Privado utilizada para fundamentar la actuación notarial consular, que crea un vínculo entre el lugar donde el acto surtirá efecto, el funcionario que lo autoriza y la forma que se debe seguir.

La regla "locus regit actum" esta reconocida en Costa Rica en el Código Civil cuando establece que "...las leyes de la República obligan a los costarricenses para todo acto jurídico o contrato que deba tener ejecución en Costa Rica, cualquiera que sea el país donde se ejecute o celebre el contrato; y obligan también a los extranjeros, respecto de los actos que se ejecuten o de los contratos que se celebren y que hayan de ejecutarse en Costa Rica."[1]

[1] Código Civil. Colección Leyes. Editorial Porvenir, 12ª. Edición, San José, 1998.artículo 23.

La regla "locus regit actum" es imperativa cuando un persona , nacional o extranjero, se encuentra en un país y realizará una acto auténtico y se dirige a un funcionario del país donde su acto surtirá efecto.

El Cónsul o el Notario Público, apegado a su ley nacional, dará autenticidad al acto, aplicando las formas que prescriben las leyes de su país, pues como expusimos existe un vínculo absoluto entre la forma empleada y el funcionario que autoriza el acto. Este principio de derecho internacional privado es reconocido plenamente por nuestra legislación civil, pues para ella "en cuanto a la forma y solemnidades externas de un contrato o acto jurídico que deba tener efecto en Costa Rica, el otorgante puede sujetarse a las leyes costarricenses..."[1]; estableciendo que cuando las leyes de Costa rica exijan un instrumento público, no tendrán valor las escrituras privadas.

Con base en esta normativa general y el reconocimiento de las normas de Derecho Internacional Privado, en nuestro país el Notario Público debidamente habilitado para ejercer, es competente para ejercer su función " en todo el territorio nacional y, fuera de él, en la autorización de actos y contratos de su competencia que deban surtir efectos en Costa Rica.[2]

---

[1] Código Civil, Artículo 28.
[2] Código Notarial, Artículo 32.

Esta autorización legal para que el Notario ejerza su función fuera de nuestras fronteras, es una situación excepcional, pues para ello se le ha concedido fe pública notarial a los Cónsules nacionales acreditados en el extranjero.

Lo anterior no significa que todos los actos autorizados por Notarios nacionales fuera de nuestro territorio, son validos y eficaces, ya que se debe estar sujeto a ciertos requisitos y condiciones que se verán a continuación.

b) Validez y eficacia de la actuación extraterritorial.

El Código Notarial establece los requisitos propios para que el Notario Público costarricense, pueda ejercer fuera del territorio nacional y su actuación sea valida y eficaz en el país.

Los requisitos o condiciones para que el instrumento notarial otorgado fuera del territorio nacional, sea válido y eficaz son:

1- Que el Notario este habilitado para ejercer la función notarial.[1]

El Notario debe cumplir con los requisitos establecidos en el Código Notarial para que la autoridad estatal competente le autorice a ejercer el Notariado, entre los cuales está el residir permanentemente y tener oficina abierta en el país. Este requisito es importante, pues si no se reside en el país, el Notario

[1] Código Notarial, Artículo 2.

estará imposibilitado de usar su Protocolo o se le suspende la vigencia de la función notarial que le deposita el Estado.

2- Autorizar actos y contratos de su competencia.

El Notario debe autorizar únicamente documentos notariales protocolares y extraprotocolares dentro de su competencia. Se debe actuar en el Protocolo autorizado por la Dirección Nacional de Notariado, ajustándose a las formalidades y limitaciones previstas en el Código Notarial.[1]

3- Autorizar actos con efectos en Costa Rica.

Que los actos y contratos que se autoricen, tengan como finalidad que su eficacia jurídica se dé en Costa Rica, sea en razón de las personas o los bienes.[2]

4- Deber de información de que saldrá del país con su Protocolo.

El Notario tiene la obligación de informar a la Dirección Nacional de Notario que lleva su Protocolo fuera del país, pues de lo contrario deberá depositarlo en el Archivo Notarial.

5- Que se encuentre dentro del plazo autorizado para cartular y/o certificar.

Una vez cumplidos todos los requisitos anteriores, el Notario podrá

[1] Código Notarial, Artículo 33
[2] Código Notarial, Artículo 32 y Código Civil, artículo 23.

autorizar actos o contratos en el extranjero siempre que no tenga más de tres meses de haber salido del país, para la utilización del Protocolo, o menos de seis meses, para mantener vigente su función notarial.

El Notario puede actuar en su Protocolo, encontrándose fuera del país, únicamente cuando se trate de una ausencia menor a tres meses, pues el Código Notarial establece que cuando el Notario se ausenta del país por más de tres meses, deberá depositar su Protocolo en el Archivo Notarial.[1]

Con respecto a su potestad actuar en conotaría y de expedir documentos extraprotocolares, encontrándose fuera del país, el Notario podrá ejercerla hasta por seis meses. Si el Notario se encuentra fuera del país por más de tres meses, conserva su función notarial hasta que cumpla seis meses, luego de lo cual se le inhabilita temporalmente, cuya suspensión se mantiene durante toda su ausencia.[2]

En este aparte es importante la clasificación de los documentos notariales analizada supra, pues para los documentos notariales protocolares, solo podrán autorizarse hasta por el improrrogable termino de tres meses cuando se realice en su propio Protocolo y hasta seis meses cuando se realice en conotaría..

[1] Código Notarial, Artículo 53.
[2] Código Notarial, Artículo 13 inciso c).

Luego de los tres meses, el Notario únicamente podrá emitir documentos notariales extraprotocolares, ya que podrá "certificar, autenticar y eventualmente, si así lo permitieran las circunstancias, puede realizar el connotariado".[1]

El Notario puede certificar cuando se encuentre fuera del país, ya que la "potestad certificadora no tiene vigencia según se trate el territorio, es una potestad que le deviene al Notario de la competencia que el Código Notarial le confiere.[2] Se podrán certificar datos que se encuentran en oficinas públicas en el extranjero, las cuales se extenderán de conformidad con las disposiciones del Código Notarial, el Código Civil y los Tratados Internacionales, manteniendo la certeza de los hechos que se certifican.

Las certificaciones serán válidas y tendrán los efectos que la ley le otorgue, en tanto y cuanto el Notario esté habilitado y cumpla con los requerimientos legales impuestos al Notario que lo autoriza y bajo los preceptos expuestos en los artículos 23 y 28 del Código Civil.

Si el Notario se mantiene fuera del territorio nacional y ha salido con su

[1] Directriz número 626-1999, de las 7:33 horas del 20 de Julio de 1999, página 5.
[2] Directriz número 626-1999, op. Cit.,página 8.

Protocolo, mantiene todas las obligaciones que le impone el Código Notarial, incluso la impuesta en el artículo 29, de presentar el índice de escrituras quincenalmente.

TITULO SEGUNDO

DE LA ACTIVIDAD INFORMATICA

CAPÍTULO I

INFORMATICA EN GENERAL

Sección I: ORIGEN Y EVOLUCIÓN DE LA RED INTERNET

A) ¿Qué es la red informática?

Durante la guerra fría, el Departamento de Defensa de los Estados Unidos de América, estaba preocupado por uno de los principales objetivos militares en caso de que se desatara una guerra nuclear. Ese objetivo era su sistema de comunicación.

A raíz de esa preocupación "se propuso un sistema de comunicaciones mediante computadores conectadas en una red descentralizada. De manera que si uno o varios nodos importantes eran destruidos, los demás podían comunicarse entre sí, sin ningún inconveniente."[1]

Este proyecto de investigación para la defensa militar, da inicio a las primeras redes de cómputo a mediados de la década de mil novecientos setenta. La primera red se llamaba ARPANET (Advance Research proyect Agencie NET) desarrollada por el Ministerio de Defensa de los Estados Unidos de América.

El objetivo de este proyecto consistía en conectar en red unas cuantas instituciones que realizaban proyectos de desarrollo de sistemas de seguridad nacional, para que en caso de un ataque nuclear nunca se interrumpiera la

[1] Historia de Internet. www,flash.net/ hejrusso/historia.htm., p.1

comunicación entre el Pentágono y los científicos de estas instituciones. Con esta red, si un enlace era interrumpido por un ataque, el tráfico se dirigía a otro. [1]

Cuando ARPANET creció, surgieron otras redes y pronto se vislumbró las necesidad de interconectarlas, por la incompatibilidad de los lenguajes o protocolos usados en las distintas redes. El Protocolo son las señales que le dicen a los dispositivos cómo comunicarse y cómo coordinar esa comunicación, de manera que dos máquinas puedan comunicarse.

> "Corría el año mil novecientos setenta y dos y con la necesidad de establecer un protocolo de comunicación común entre todas las computadores, que variaban en tipo y sistemas operativos (IBM y Unisys, por nombrar algunas), para que pudieran comunicarse entre sí, sin ningún inconveniente, se crea el InterNetworking Working Group."[2]

En el año mil novecientos setenta y ocho este problema de incompatibilidad de las distintas redes se solucionó con la adopción del protocolo TCP/IP (Transmisión Control Protocol / Internet Protocol: Protocolo de Control de Transmisión / Protocolo Internet) en la cual se basa toda la red internet, por ser el lenguaje en el que se comunican los computadores.

---

[1] AGUILAR SÁNCHEZ (Edwin). El Comercio Electrónico. Curso de Nivel Superior sobre Comercio Electrónico. Instituto Costarricense de Administración Pública, San José, Enero-Febrero, 2000.
[2] Historia de Internet. Op.cit, p.1

Con el uso del protocolo TCP/IP, ARPANET crece y se le unen otras redes existentes como los eran la CSNET o BITNET, hasta que la parte de la red involucrada con el ejército se separa en mil novecientos ochenta y dos y crea su propia red llamada MILNET. Este hecho se toma como referencia para el nacimiento de INTERNET.[1]

Paralelamente a los esfuerzos militares, la National Sciencie Foundation NSF crea una red para enlazar cinco centros que poseían supercomputadoras en distintas ciudades de los Estados Unidos para poder dar acceso a los investigadores que en ella se encontraban, desarrollándose con ello la NSFNET, en mil novecientos ochenta y siete.

En esta época surgía la CERN (European High Energy Particle Physics Lab), que era el mayor centro de Internet en Europa, donde nace el World Wide Web conocido mundialmente por sus siglas WWW. Este sistema se basaba en dos aspectos: el desarrollo del HTML (Hypertext Markup Language); y el Protocolo HTTP (Hipertext Transfer Protocol), que hicieron posible el trabajo en redes. [2]

El empleo de la WWW permite a los usuarios "navegar" por la información gracias a las palabras activadas en el hipertexto que conducen de manera

---

[1] Historia de Internet. Op.cit. p.1.
[2] BOGARIN NAVARRO (Rodrigo) Descubra el mundo de Internet, San José, Costa Rica, Editorial Tecnológica de Costa Rica, 1era. Edición, 1995, p.18.

automática a otra referencia, ya sea del mismo archivo, o bien de archivos situados en otros servidores de otras partes del mundo.

Cuando en mil novecientos noventa ARPANET es desactivada, la NSFNET sustituye sus servicios, pero no resultó exitosa debido al alto costo de las máquinas, lo que provocó la búsqueda de equipos más sencillos con alta capacidad de desempeño. Este hecho permitió el desarrollo y crecimiento de INTERNET, que es ese momento se limitó a la conexión de redes pequeñas entre sí.[1]

Actualmente INTERNET es una red de redes de computadoras a nivel mundial, que se interconectan con el protocolo TCP/IP, por lo que algunos le han llamado la "supercarretera de información".

Internet es definida por el Consejo Federal de Redes (The Federal Networking Council -FNC) en una resolución que indica: "Internet se refiere al sistema global de información que está: (i) lógicamente unido entre sí, por una dirección espacial global única, basada en el protocolo Internet (IP) o sus extensiones subsecuentes; (ii) es capaz de soportar comunicaciones usando el protocolo de control de transmisión (TCP/IP) o sus extensiones subsecuentes, u otros protocolos IP compatibles, y (iii) provee, usa o hace accesible, ya sea pública

[1] Historia de Internet, p.2

o privadamente, servicios de alto nivel establecidos en las comunicaciones e infraestructura descritas aquí."[1]

Douglas E. Comer describe Internet de la siguiente manera: " Internet es una biblioteca digital global, intensa y exitosa, de rápido crecimiento, estructurada sobre una tecnología de comunicación notablemente flexible. La biblioteca digital de Internet ofrece una variedad de servicios que se utilizan para crear, explorar, acceder, buscar, ver y comunicar información sobre un conjunto diverso de temas, que abarcan desde resultados de experimentos científicos hasta discusiones sobre actividades recreativas. La información en la biblioteca digital de Internet puede ser grabada en memorándums, organizada en menús, almacenada en documentos de hipermedios o en documentos de texto. Además, la información, accesible a través de la biblioteca digital, puede consistir en datos, incluyendo audio y video, reunidos, comunicados y distribuidos en forma instantánea sin necesidad de almacenarse. Por otra parte, dado que los servicios están integrados y poseen referencias cruzadas, el usuario puede moverse de manera uniforme y continua de la información de una computadora a otra, y de un servicio de acceso a otro."[2]

No importando la definición que se adopte en cuando a Internet, lo cierto es que su crecimiento ha sido constante desde su nacimiento, veamos:

---

[1] http::/www.isoc.org/internet/history/brief.htm

[2] COMER (Douglas E.) El libro de Internet, Segunda Edición, Prentice- may, México, 1998, p. 271.

A) En 1997 existían 19.5 millones de hosts (servidores) y 1.3 millones de sitios de dominio;

B) Para 1998 el número de hosts creció en un 128% y el número de dominios registrados creció en 137%.

C) En cuanto al número de usuarios de Internet entre 1998 y Mayo de 1999 su número creció en 55%, llegando a ser 171 millones.[1]

Por su constante crecimiento de usuarios y por su propia naturaleza, Internet aparece como una herramienta de negocios en 1995. Algunos aspectos que la llevaron a ello, los podemos determinar básicamente en que:

a- Cada vez atrae más cantidad de personas de todos los países, edades, culturas, e idiomas que tienen fines diversos al utilizar la red, como pueden ser información, negocios, investigación, entretenimiento, política, negocios, etc.

b- Es muy popular en la población educada por su capacidad para comunicarse globalmente en forma instantánea, permitiendo todas las formas de expresión en una interfase amigable: el World Wide Web (www).

c- Su desarrollo técnico ha sido guiado por protocolos abiertos de dominio público, lo que la hace más accesible a más personas.

---

[1] AGUILAR SÁNCHEZ (Edwin). El Comercio Electrónico, Op.cit, p.9

d- No tiene una autoridad o control central. Se desarrolla de manera descentralizada y autónoma, siguiendo políticas y regulaciones generales. Para el uso y registro de Nombres de Dominio, se cuenta con una institución responsable denominada;: Internet Corporation for assigned Names and Numbers, (ICANN).

e- Es multijurisdiccional y traspone la históricas barreras de las fronteras. Los usuarios pueden accesarla desde cualquier lugar de la Tierra y la información viaja a través de varios países y jurisdicciones para llegar a su destino.

f- Esta en permanente evolución, pues actualmente se está desarrollando el internet 2 y los protocolos se desarrollan bajo la presión tecnológica, como por ejemplo el bluetooth, para el acceso inalámbrico.[1]

Estos aspectos que conforman la naturaleza propia de la Internet, es lo que hace que sea propicia para el comercio al detalle, llevando ventaja al comercio tradicional por su velocidad y bajo costo, lo cual da inicio a una verdadera economía digital.

[1] AGUILAR SÁNCHEZ (Edwin). El Comercio Electrónico, Op. Cit., página 8.

Como medio de información para el comercio, es el medio que ha alcanzado más usuarios en menos tiempo, veamos: Para alcanzar 50 millones de usuarios a la radio le tomó 38 años, a la Televisión le tomó 16 años y a la Internet le tomó tan solo 4 años.

Es por esa facilidad de acceso a la información que es pieza fundamental para el comercio, superando su crecimiento real a las expectativas y proyecciones que se tenían. Por ejemplo: en ventas al detalle, el comercio por Internet generó en 1998 la suma de quince millardos y se espera que para el 2002 esa suma alcance entre cuarenta u ochenta millardos.[1]

El uso de Internet en el comercio, ha traído un cambio en la cadena de producción, ya no es tierra, capital y trabajo, sino información y conocimiento. Cuando se identifica la necesidad de los clientes se procede al diseño, se compran los materiales necesarios, se manufactura, se hace el mercadeo, venta, distribución y servicios. El proceso de producción no es secuencial, pues el servicio se da en todas las etapas del proceso y el diseño no es solo del producto, sino de todas las etapas del proceso.

B) Servicios que presta.

---

[1] AGUILAR SÁNCHEZ (Edwin).Economía Digital. Curso de Nivel Superior, impartido en el Instituto Centroamericano de Administración Pública, ICAP, San José, Enero-Febrero, 2000.

El crecimiento de la red a sido tan impresionante, que actualmente se puede realizar casi cualquier operación en Internet, como por ejemplo: ver publicaciones, comprar libros, flores, autos, discos, computadoras, zapatos, casas, etc. La adopción de "browsers" (exploradores o visualizadores) y los WWW, permiten a los usuarios un fácil acceso a la información, por lo que todo esta a un click de distancia.

Dentro de los principales servicios que se reciben de Internet están como dijimos el WWW, el correo electrónico, la transferencia de archivos FTP (File Transfer Protocol), la búsqueda de archivos (Archie), localización de personas, conversaciones, consulta de noticias, etc.

De todos los servicios que brinda Internet, dos son los más utilizados por los usuarios: **la WWW y el Correo Electrónico**.

i- La www (World Wide Web)

Son una colección de páginas electrónicas que se encuentran en la red de Internet y que están ubicadas alrededor del mundo. Como expusimos anteriormente, se basan en el hipertexto, aunque actualmente con el avance tecnológico y de la multimedia, se le ha incorporado la posibilidad de tener video, música y programas interactivos, que las hacen más atractivas, amigables y sencillas para navegar.

El acceso a estas páginas electrónicas ser realiza mediante un programa o aplicación (software) denominado "browser" que permite la visualización de páginas del Web, lo que agiliza el tiempo de búsqueda de un tema particular. Estos "browsers hacen posible el traslado casi instantáneo de un página electrónica del lugar donde se encuentra, a la pantalla del computador del usuario que la quiere acceder y que lo ha realizado mediante la conexión a un hipertexto o vínculo.[1]

Estos visualizadores o exploradores han superado en cobertura y alcance a GHOPER, que eran los que anteriormente se utilizaban para la localización de información que permitía interconectarse a Internet. Si el usuario selecciona un tema que corresponda a un menú de ghoper, el sistema deja temporalmente WWW y usa ghoper para presentar el menú; cuando el usuario termina con ghoper, el sistema regresa al documento de hipermedios de WWW.

Existen varios exploradores en la red, pero los más utilizados son el Internet Explorer y el Navigator Netscape, entre los cuales se da una gran competencia que los especialistas han denominado una verdadera guerra para acaparar a los cibernautas.[2]

---

[1] Vía Internet (Revista) Año 1, número 1, San José, Agosto del 1997, página 9.
[2] RUPLEY (Sebastián) La Guerra del Web. PC Magazine en español. Documento sin año, página 62.

ii- Correo Electrónico o e´mail.

Cada usuario (persona física, grupo u organización) tiene una dirección de correo electrónico, similar al apartado postal del correo ordinario, desde donde envía y recibe correspondencia trasmitida electrónicamente. La correspondencia electrónica ingresa a un buzón asignado, donde también deposita los mensajes que desea enviar, lo cual se realiza de manera rápida, fácil y económica.

No existen dos direcciones de correo electrónico iguales en todo el mundo, por lo que existe seguridad de que los mensajes son recibidos por la persona a quien le ha sido asignada dicha dirección.[1] Estas direcciones se componen de dos parte: un login o identificador y el nombre del computador y dominio al que pertenece el usuario, separada ambas partes por el símbolo "@".

La agilidad de este servicio de Internet, hace que además de enviar mensajes de texto, se puedan adjuntar cualquier tipo de archivo. Esto es lo que se conoce con el nombre de "attachment", donde se pueden enviar cualquier tipo de información con imagen, gráficos, sonidos, etc.

Esta gran variedad de posibilidades y la rapidez de la información de la comunicación, hacen que actualmente sea imposible sustraerse a este tipo de servicio de la red.

---

[1] http::/www.isoc.org/internet/history/brief.htm

C) Usos y posibilidades.

Prácticamente es difícil determinar los usos y posibilidades de la Internet, ya que no se conocen límites para la red.

Hemos visto la utilidad del correo electrónico, de la WWW y dentro de este la utilización de los browsers para la búsqueda de los temas que el usuario requiera del mar de información existente en red.

Cuando los servidores se llenaron de información, fue necesario que se construyera un programa que por sí solo buscara en la red, los documentos donde existieran palabras claves que se hubieran digitado. Fue así como iniciaron los robot de búsqueda o buscadores[1]

Los buscadores funcionan con una serie de palabras que se les digita y ellos se encargan de buscar en sus bases de datos, para devolver las direcciones en donde encuentran esas palabras. Algunos de los robots de búsqueda permiten también buscar por temas como por ejemplo; salud, ciencia, deportes, etc. Los buscadores más conocidos en red son: Yahoo, Alta Vista, Hotmail, Lycos, etc.

Internet es una herramienta para adquirir conocimiento y quienes tienen acceso a dicho conocimiento, son los que tendrán sus bolsillos llenos, puesto que

[1] http://www. la nación.com Reportaje Juan Fernando Lara, Búsqueda fácil en internet, p.2.

se han superado los viejos dogmas de la era industrial que no se adecuan a los hechos actuales, donde los datos y la información adquieren un enorme valor.

Como expusimos supra, se da un cambio en la cadena de producción, pues el valor agregado es información en todas las etapas del proceso.

Se da un cambio sustancial en la cadena de valor, pues además de los recursos humanos, los insumos, la tecnología y los activos financieros que se mueven en la cadena física, en la cadena virtual se mueve información en todos los puntos, lo que da mucha ventaja competitiva en el mercado.[1]

En la era de la información se deja atrás la producción en masa de las grandes empresas y se pasa la era de la producción por demanda (massive customization). El capital será manejado por las personas que manejan la información, quienes aportaran el conocimiento como un valor agregado en el mercado.

El uso y las posibilidades de los usuarios de Internet es inimaginable: por un lado los usuarios tienen toda la información necesaria de los bienes y servicios justos a su medida (hay mayor capacidad para escoger, se ahorra tiempo, se tiene más comodidad, en el horario que quiera y al precio que mas le convenga); y por

[1] AGUILAR SÁNCHEZ (Edwin) Economia Digital, Op.cit.

otro lado, los empresarios tienen un alza en sus ventas por los nuevos nichos que se dan en el mercado global, reduciéndose sus costos de operación.

La reducción de costos en la producción se da porque el empresario tiene el conocimiento preciso de lo que requieren los usuarios, información que los propios usuarios dan en la red, por ejemplo Amazon no solicitará un tiraje de libros que no sabe si va a vender, sino que solicitará el tiraje dependiendo de las personas que visiten su sitio web y lo requieren, lo cual bajo sus costos de producción.

Además las posibilidades de Internet en cuanto a la aplicación del conocimiento en la reestructuración de la organización, logra que las empresas bajen sus costos, tal como lo hizo la empresa Texas Instruments, que al automatizar sus ordenes de compra pasaron de un costo de $49.0 a $ 4.70.[1]

Pero las posibilidades no son únicamente para los grandes empresarios, sino también para cualquier persona que quiera abrir su propio sitio en la red o enviar la información a un sitio contratado para poner en red el servicio o bien que desea negociar.

Como se expuso, también los usuarios tienen un mercado virtual tan amplio como la red misma, el cual se encuentra al alcance de su mano. Sin duda alguna Internet es una gran mall virtual donde se compra todo tipo de bienes y servicios.

---

[1] PEREZ MERAYO (Guillermo). La Informática y la Política. Hacia un Gobierno Electrónico. Revista Electrónica de Derecho Informatico, www.derecho .org Febrero, 2000, sin número de página

Desde confites hasta vehículos Ford o Land Rover, pasando por tiquetes aéreos, hoteles, medicamentos, entretenimiento, etc.

SECCION II: PROTOCOLOS DE INTERNET.

A) Capas (Internas y externas)

Como se conoce, Internet es una red de redes independientes. Una red permite conectar a los ordenadores que la forman con la finalidad de compartir información, bases de datos, o recursos físicos.

Desde los inicios de Internet se dieron muchas redes independientes, las cuales suelen clasificarse según su extensión.

Primero se inicio con las redes LAN (Local Area Network), que eran redes de área local. Las primeras LAN se utilizaron para interconectar las computadoras de un mismo departamento de una empresa, por lo que su extensión suele estar restringida a una sala o edificio, aunque también podría utilizarse para conectar dos o más edificios próximos. [1]

[1] COMER (Douglas E.) El Libro de Internet. pp. 49-50

Las redes LAN no son de la misma tecnología, ya que ello depende de las necesidades del grupo dentro de la empresa que puede ser determinada por el costo, la velocidad, la facilidad de instalación o el mantenimiento; es por ello que es posible encontrar que dos grupos de una empresa elijan diferentes tecnologías LAN.

El problema de las tecnologías LAN es que algunas son completamente incompatibles por su diseño de longitud de cable, por sus especificaciones eléctricas o por la manera de codificar la información.[1]

Una red más extensa son las redes de área amplia o WAN (Wide Area Network). Son redes que cubren un espacio muy amplio, conectando a ordenadores de una ciudad o un país completo, utilizando las líneas de teléfono y otros medios de transmisión más sofisticados, como pueden ser las microondas.

Es así como varias redes pueden conectarse entre sí formando una red lógica de área mayor. Para que la transmisión entre todas ellas sea posible se emplean los "routers" y los "gateway", que son los sistemas que conectando físicamente varias redes se encargan de dirigir la información por el camino adecuado y conectan las redes de diferente tipo y con protocolos distintos.

---

[1] Idibem, página 51.

El problema de la incompatibilidad de las redes hizo necesario un sistema en la red que permitiera que esas redes se comunicaran entre sí en un solo lenguaje.

Para que todas estas redes se puedan interconectar y acceder a la información que cada una tenga, se diseño la tecnología del software que contiene muchos programas computaciones complejos que funcionan juntos para realizar la comunicación.

Este software conocido como TCP/IP (Protocolo de Control de Transmisión/Protocolo Internet), define normas que hacen posible la comunicación de dos redes con equipos y dispositivos distintos mediante un protocolo que especifica el lenguaje común que utilizan dos computadoras para intercambiar mensajes. [1]

Todo computador conectada a Internet, excepto los routers, capaz de compartir información con otro computador se conoce con el nombre de host (anfitrión o servidor), que se identifica y dispone de una dirección única y exclusiva. Esta dirección, conocida como dirección de Internet o dirección IP, es un número de 32 bit que generalmente se representa en cuatro grupos de 8 byte

[1] COMER (Douglas E.) El Libro de Internet. Op.cit. p. 107

(octetos) cada uno separados por puntos y en base decimal.[1] Por ejemplo la dirección IP de una computadora podría ser: 128.10.2.1

El lenguaje de las computadoras es un sistema de impulsos eléctricos, mediante el cual se codifican y descodifican todas las operaciones y procesos, donde la máquina entiende una larga serie de ceros y unos; el cero equivale a ausencia de corriente y el uno indica el paso de corriente.

La unidad mínima de información es un bit, que será un cero o un uno, el cual no es plenamente significativo, pero al agruparlos en ocho bits se constituye un byte .

Las combinaciones posibles de los dígitos del sistema binario en un byte permiten doscientas cincuenta y seis formas posibles, a cada una de las cuales se le puede asignar un símbolo, letra o número. La codificación más extendida de este tipo es el llamado código ASCII (American Standard Code for Informatión Interchange- Código Estándar Americano para el intercambio de Información.) [2]

La arquitectura de Internet esta basada en un modelo de capas, que hace más fácil implementar nuevos protocolos para la interconexión de sistemas abiertos.

---

[1] GORDO SAEZ (Roberto). La transmisión de información en Internet. http// **www.bachillerato.uchile.cl**, 1998, documento sin numeración.

[2] Enciclopedia Autodidáctica Interactiva Océano, Volumen 6, Océano Grupo Editorial S.A. Barcelona, 2000, p. 1545

La Organización Internacional de Normalización creó un modelo denominado OSI (Open System Interconection), que es utilizado por prácticamente la totalidad de las redes del mundo.

Este modelo consiste en siete capas, cada una de las cuales define las funciones que deben proporcionar los protocolos para intercambiar información entre varios sistemas y permite que cada una tenga una finalidad determinada.

Cada capa depende de las otras, pues cada capa inferior proporciona alguna funcionalidad a las de nivel superior.

Los siete capas del modelo OSI son los siguientes:

1- Aplicación: Destino final de los datos para el usuario.

2- Presentación: Interpretan los datos que se utilizarán en la aplicación.

3- Sesión: Encargo de aspectos de comunión como el control de los tiempos.

4- Transporte: Encargada de que la información llegue de manera fiable y correcta a su destino.

5- Red: Encamina los datos hacia su destino eligiendo la ruta más efectiva.

6- Enlace: Controla el flujo de los datos, la sincronización y los errores que puedan producirse.

7- Físico: Se encarga del medio de transmisión o el hardware.[1]

Como dijimos el TCP/IP es el protocolo común más utilizado por todos los ordenadores conectados a Internet, que cuentan con hardware y software que en muchos casos son incompatibles, aunque no es el único protocolo. En realidad lo que se conoce como TCP/IP es un conjunto de protocolos que cubren todas las siete capas OSI mencionadas.

En Internet se diferencian cuatro niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

1- Aplicación: Corresponde a los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y el protocolo HTTP (Hypertext Transfer Protocol).

[1] GORDO SAEZ (Roberto) Op.cit.

2- Transporte: Al igual que en OSI, los protocolos de este nivel (TCP y UDP) se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

3- Internet: Nivel de red utilizado por el nivel de transporte que incluye al protocolo IP, encargado de enviar los paquetes de información a sus destinos correspondientes.

4- Enlace: Realiza las funciones de Enlace y Físico descritos en las capas OSI. Está encargado de la transmisión a través del medio físico al que se encuentra conectado cada servidor. [1]

En este nivel de Internet los protocolos utilizados pueden ser muy diversos y no formar parte del conjunto TCP/IP, pero una de las funciones de este protocolo es intercambiar información entre medios diferentes y tecnologías que inicialmente son incompatibles.

[1] MIRAVET BONET (Juan Salvador). Protocolos TCP/IP. **Al019803@alumail.uji.es**, 1999. Documento sin numeración.

B) Transmisión Control Protocol/Internet Protocol.

i- TCP (Transmisión control Protocol)

En TCP la transmisión de datos en Internet se realiza en unidades de poco tamaño o paquetes que reciben el nombre de "datagrama", que son conjuntos de datos que se envían como mensajes independientes, lo que proporciona grandes ventajas en la transferencia y en el manejo de los mismos.[1]

El protocolo de control de transmisión (TCP) pertenece al nivel de transporte, siendo el encargado de dividir el mensaje original en datagramas de menor tamaño mucho más manejables, que son dirigidos a través del protocolo IP de forma individual. El datagrama viaja a través de Internet de manera independiente del servidor que lo envió, por lo que este puede reanudar sus tareas una vez que el paquete inicia el viaje.

El protocolo TCP se encarga además de añadir cierta información necesaria a cada uno de los datagramas. Esta información se añade al inicio de los datos que componen el datagrama en forma de cabecera.

[1] MIRAVET BONET (Juan Salvador) Op.cit.

La cabecera de un datagrama contiene al menos 16 bits que se encuentran repartidos en varios campos con diferente significado. Cuando la información se divide en datagramas para ser enviados, el orden en que éstos lleguen a su destino no necesariamente tiene que ser el correcto. Cada uno de ellos puede llegar en cualquier momento y con cualquier orden, e incluso puede que algunos no lleguen a su destino si un ruteador se desborda o que lleguen con información errónea. Para evitar todos estos problemas el TCP numera los datagramas antes de ser enviados, de manera que sea posible volver a unirlos en el orden adecuado o permite también solicitar de nuevo el envío de los datagramas individuales que no hayan llegado o que contengan errores, sin que sea necesario volver a enviar el mensaje completo.[1]

El formato de la cabecera del TCP tiene dos campos con un puerto de origen y un puerto de destino con una longitud de 16 bits, los cuales distinguen las distintas y simultaneas transferencias que un mismo servidor esté utilizando.

Después están los números de secuencia (SSN) tienen 32 bits y los de reconocimiento o confirmación, que envía la señales cuando se ha recibido la información satisfactoriamente. Por razones de eficiencia los datagramas se envían

[1] COMER (Douglas E.) El Libro de Internet. Op. Cit. pp.1107-111.

continuamente sin esperar la confirmación, haciéndose necesaria la numeración de los mismos para que puedan ser ensamblados en el orden correcto.

Posteriormente encontramos la longitud de cabecera, el control de bits, las ventanas que regulan las cantidad de información que el receptor está preparado para procesar; el relleno o padding y el checksum que garantiza la integridad del mensaje, comprobando que es el mismo que el suministrado en la cabecera.[1]

Además del TCP que es el protocolo más utilizado para el nivel de transporte en Internet, existen otros protocolos como el UDP, que no admite numeración y se utiliza cuando el orden de los datagramas no es fundamental y el ICMP que tiene un formato más simple y se utiliza en los mensajes de error y de control necesarios para los sistemas de la red.

ii- IP (Internet Protocol) versión 4.

El IP es un protocolo que pertenece al nivel de red, es utilizado por los protocolos del nivel de transporte como TCP para encaminar el datagrama hacia su destino. No comprueba la integridad de la información, únicamente lo transporta, para lo cual utiliza una nueva cabecera.

---

[1] MIRAVET BONET (Juan Salvador). Op.cit.

El IP al igual que el TCP, está compuesto de varios segmentos, a saber:

@ La cabecera IP con un valor de cuatro bits, que tendrá su propia longitud (Internet Header Length) la cual también contiene cuatro bits.

@ El tipo de servicio especifica la prioridad de los datos que se envían, tendrá un tamaño de ocho bits.

@ La longitud total es la longitud en bytes del datagrama completo, incluyendo la cabecera y los datos.

@ La identificación es el número secuencial asignado por el servidor de origen, que combinado con la dirección del host forman un número único en la red.

@ La Fragmentación offset se da cuando el tamaño del datagrama excede el hardware que se utilice para su transmisión, para poder ensamblarlos nuevamente.

@ Los Flags son los indicadores utilizados en la fragmentación del mensaje.

@ El Limite de existencia o tiempo de vida es el segmento que representa los segundos que un datagrama puede existir en Internet antes de ser descartado.

@ Protocolo es el segmento que indica a cual de todos los protocolos pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino.

@ Por último está el campo de comprobación (checksum) es necesario para verificar que los datos contenidos en la cabecera IP son correctos y dar seguridad de que el datagrama no ha sido dañado ni modificado.

@ Por último en la configuración del IP versión cuatro, encontramos la dirección de origen o sea la del host que envía el paquete o datagrama y la dirección de destino que es la del host que lo recibirá. [1]

En todo este esquema los campos deben ser conocidos por los routers o gateway intermedios, para dirigir correctamente el paquete.

El protocolo IP que identifica a cada ordenador se encuentra conectado a la red mediante su correspondiente dirección, la cual es un número de 32 bit que debe ser único para cada host, y normalmente suele representarse como cuatro cifras de 8 bit separadas por puntos.

[1] GORDO SAEZ (Roberto). Op.cit.

C) IP (Interneto Protocol) VERSION 6.

La versión 6 del protocolo IP que recibe el nombre de IPv6, también conocida como IPng (Internet Protocol Next Generation), es la más nueva versión del IP 4.

Se debe aclarar que no hubo IP5, que no pasó de su fase experimental.

Las modificaciones introducidas en la versión 6 son muchas y de gran importancia, encaminadas a mejorar la seguridad en la red, ofrecer soporte a las nuevas redes de alto rendimiento (como ATM, Gigabit Ethernet, etc. y solucionar algunos problemas surgidos en la versión anterior.[1]

Una de las características de IPng es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bit, eliminando todas las restricciones del sistema actual.

El nuevo formato de la cabecera, aunque ocupa el doble de la anterior versión, se ha organizado de una manera más efectiva; se omitieron algunos campos y otras son opcionales, permitiendo que las opciones se sitúen en

[1] MIRAVET BONET (Juan Salvador) Op.cit.

extensiones separadas de la cabecera principal y que los routers no tengan que procesar tanta información.[1]

El formato completo de la cabecera de esta versión, sin las extensiones, es el siguiente:

@ El número del protocolo IP, que en este caso contendrá el valor 6.

@ El segundo campo contiene el valor de la prioridad o importancia del paquete que se está enviando con respecto a otros paquetes provenientes del mismo servidor.

@ Posteriormente llega una etiqueta de flujo que indica que el paquete requiere un tratamiento especial por parte de los routers.

@ El siguiente campo es la longitud que precisamente indica la longitud en bytes de los datos que se encuentran a continuación de la cabecera.

@ El formato continúa con la siguiente cabecera, que se utiliza para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual.

---

[1] GORDO SAEZ (Roberto) Op.cit.

@ El límite de existencia tiene el mismo propósito que el campo de la versión 4, y es un valor que disminuye en una unidad cada vez que el paquete pasa por un nodo.

@ Los últimos campos son uno de los cambios más importantes de la versión 6 y que están designados para la dirección de origen y la dirección de destino, que son cuatro veces mayor que la versión cuatro; pasan de 32 a 128 bytes.[1]

"Las extensiones que permite añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. Los datos situados en cabeceras opcionales se procesan sólo cuando el mensaje llega a su destino final, lo que supone una mejora en el rendimiento. Otra ventaja adicional es que el tamaño de la cabecera no está limitado a un valor fijo de bytes como ocurría en la versión 4."[2]

Esta versión de IP tienen tres tipos básicos de direcciones:

a) Las direcciones unicast dirigidas a un único interfaz, compatible con las direcciones del IP4;

[1] MIRAVET BONET (Juan Salvador). Op.cit.
[2] GORDO SAEZ (Roberto), Op.cit.

b) Las direcciones anycast, que son unicast designadas a un conjunto de interfaces de la red, que envían el paquete a cualquiera de ese conjunto; y

c) Las direcciones multicast que identifica a un conjunto de interfaces de la red, de manera que el paquete es enviado a cada una de ellos individualmente. [1]

SECCION III: SEGURIDAD EN INTERNET.

Uno de los temas que más preocupan a los usuarios de Internet, en cuanto a la privacidad de la información, es el de la seguridad.

Las computadoras y las redes de datos necesitan de ciertas precauciones que ayuden a mantener segura la información, la cual tiene un valor significativo.

La seguridad de los web-sites preocupa al 80% de los usuarios de Internet y la asocian al uso de las tarjetas de crédito o debito. La privacidad de la información personal y su uso por las empresas Internet, preocupa al 84% de los usuarios y la asocian al uso comercial de la información financiera y médica.[2]

---

[1] MIRAVET BONET (Juan Salvador), Op.cit.

[2] Esta información se encuentra en el sitio **www.jupiter.com**, en referencia a los servicios de planificación de estrategias (SPS- Strategic Planning Services)

Por un lado está el desarrollo de la seguridad de red, que se refiere al nivel de confiabilidad de los usuarios en las políticas de la red en cuanto al manejo de la información y el de la seguridad de la información para que no sea accesada por usuarios no autorizados.

La seguridad de la red está referida tanto a la protección de física de la infraestructura, pero lo más importante es la protección de la integridad de los datos y la disponibilidad de los mismos, esto incluirá la protección de cambios no autorizados, evitar que desde el exterior se evite el acceso a la información y evitar lecturas no autorizadas.[1]

Hay que tomar en cuenta que cuando hablamos de seguridad en red, no solamente se trata de los dispositivos del usuario que envía y del que recibe, sino que se introducen terceras partes que son las que controlan cómo se procesan y rutean los paquetes de información.

Las funciones de seguridad no las trataremos técnicamente, sino únicamente realizaremos una explicación para posteriormente retomaremos en el desarrollo del tema principal donde son de suma importancia para la firma digital.

---

[1] COMER (Douglas E.) Introducción al Estudio del TCP/IP, Prentice-Hall, México, 1997, p. 480

A) La Criptología.

La Criptología es el estudio de la seguridad de las comunicaciones y de las técnicas para descifrar las comunicaciones secretas. "Trata de métodos y técnicas de encripción y decripción de comunicaciones, al servicio de la seguridad, la autenticación, la identificación, la firma digital y servicios varios".[1]

La Criptología es muy importante al analizar las principales funciones de seguridad, que podemos resumir en lo siguiente:

a) Identificación-Autenticación de las partes: Se debe garantizar que los sujetos cuya información se cruza o que transan, sean realmente quienes se espera que sean. Esto se le conoce como autenticidad no repudiable.

b) Integridad del mensaje: Garantizar que el contenido del mensaje no ha sido cambiado durante su tránsito por la red o durante su almacenamiento.

c) Certidumbre de la transacción: Garantizar que la transacción o respuesta ha sido originada por una parte, con pleno conocimiento y aceptación de la otra. Debe existir una evidencia cierta, lo que se denomina no repudiable/ no

[1] AGUILAR SÁNCHEZ (Edwin), Economía Digital. Op.cit.

refutable. Ninguna de las partes puede decir que no ocurrió lo que ocurrió.

d) Prueba irrefutable de la fecha (time stamping): Se aporta evidencia irrefutable de la fecha y hora de la transmisión.

e) Privacidad: Garantiza que la información sensible de una parte sólo será conocida por otra parte legitimante autorizada o llamada a procesarla.

f) Por último esta la encripción del mensaje, que consiste en codificar la información mediante un proceso matemático o algoritmo (hash) para hacerla ininteligible a todos, excepto al destinatario legítimo.[1]

Este proceso matemático (algoritmo) necesita de una clave, de tal forma que al aplicar el mismo algoritmo a un texto con claves diferentes, el resultado es diferente y único para cada clave.

Hay niveles de encriptación dependiente del largo de clave o llave que se utilice.

Las encripciones en protocolo abierto a nivel del web server, como son el https y el SSL (Secure Socket Layer).

---

[1] AGUILAR SÁNCHEZ (Edwin) Economía Digital. Op.cit.

Otro nivel de seguridad lo da el SET (Secure Electronic Transactions), el cual es un protocolo propietario por lo que el servidor debe enviar el software para instalarlo.

El Protocolo SET es un conjunto de especificaciones que fue desarrollado para permitir las transferencias y pagos por Internet a cualquier otra red.

El SET realiza una combinación de métodos criptográficos que garantizan la confidencialidad, la autenticidad de las parte, la integridad del documento y el no repudio de la misma, lográndose una transacción perfecta.[1] Es este nivel de aplicación de seguridad que se utiliza cuando realizamos una compra en Internet y cancelamos con nuestra tarjeta VISA.

La encripción se basa en dos elementos cruciales: un procedimiento o función matemática (algoritmo) y una clave o llave.

Al considerar el proceso de encripción y su correspondiente desencripción, surgen dos tipos de sistemas: sistemas simétricos y sistemas asimétricos.

[1] RAMOS SUAREZ (Fernando). Protocolo SET. Revista Electrónica de Derecho Informático. **www.derecho.org.**, p. 1.

B) CLAVES Y LLAVES (Sistema Simétrico-Sistema Asimétrico)

i) Sistema Simétrico:

En los sistemas simétricos la clave utilizada para decifrar es la misma que la que se utilizó para cifrar (o es una variación directa de ella).

En este sistema la seguridad está en la forma de trasmitir la llave, pues el usuario debe poseer el algoritmo de encriptación (programa) y su clave personal, la cual distribuye a las personas que se pretende enviar mensajes encriptados, para que ellos utilicen esa clave para desencriptar.[1]

Los principales algoritmos utilizados de encriptación simétrica son: DES (Data Encryption Standard), 3DES (o Triple DES), IDEA (International Data Encryption Algorithm), RC2, RC4 y Blowfish.

Este método tiene el problema de que alguien puede interceptar el envío de la clave, con la cual podrá leer todos los mensajes que se envíen con esa clave y accesar al texto por lo que no se puede autenticar ese mensaje.

ii) Sistema Asimétrico:

Este sistema tanto el emisor como el suscriptor usan dos claves en una única operación criptográfica: una clave pública que sirve para cifrar el mensaje de

[1] GONZALEZ T. (Patricio) VILLALÓN I. (Álvaro). Introducción a la Criptografía. Revista Electrónica de Derecho Informático. 1999. **www.derecho.org**, documento sin numeración

datos, y una clave privada para descifrarlo. De esta manera, un mensaje codificado con una clave pública determinada, solamente podrá descodificarse con la clave privada correspondiente y viceversa.[1]

Lo importante en este proceso es que la clave privada sólo la conoce el usuario propietario de ella, y es la pública la que se distribuye para que el resto del mundo la utilice para enviarnos mensajes, si alguien capta el mensaje no podrá descifrarlo ya que sólo se descifra con la clave privada que está en nuestra posesión.

Este proceso provee confidencialidad del mensaje, cuando se encripta con la llave pública y autenticidad del autor del mensaje porque se encripta con la clave privada. Con este mecanismo se soluciona el problema de tener que comunicar la clave privada, pues sólo las claves públicas son divulgadas sin riesgo con lo que se aumenta la seguridad del sistema.

Los principales Algoritmos de Criptografía asimétrica que se utilizan son: RSA (Rivest-Shamir-Adelman), DSS (Digital Signature Standard), y ECC (Elliptic Curve Criptography)

Para evitar problemas de que el mensaje de datos se envíe a la persona equivocada, surgen las Autoridades de Certificación (CA) que verifican la

---

[1] GONZALEZ T. (Patricio) VILLALÓN I. (Alvaro). Op.cit.

identidad de los usuarios y les acredita un "certificado digital" o "Digital ID", que da la seguridad de la identidad de los usuarios.

El tema de las Autoridades Certificadoras, los distintos tipos de Certificado Digital y la integridad de los mensajes envidos en red, se tratará con más amplitud en el desarrollo del tema del documento informático.

C) MUROS DE SEGURIDAD (FIREWALLS)

El control de acceso a la red se ha establecido mediante bloques conocidos como "muros de seguridad" o "firewalls", en la entrada hacia la parte de la red que será protegida.

"Un sistema de firewall es un conjunto de componentes hardware y software destinados a establecer unos controles de seguridad en el punto o puntos de entrada de nuestra red."[1]

Un muro de seguridad bloquea todas las comunicaciones no autorizadas entre las computadoras del interior y las del exterior.

---

[1] GONZALEZ T. (Patricio) VILLALÓN I. (Alvaro). Op.cit.

Con este sistema se puede llegar donde los mecanismos de seguridad de los sistemas operativos a veces no pueden, permitiendo ofrecer y utilizar servicios de Internet de forma más segura.

Para que los muros de seguridad sean eficientes y no afecten el nivel de servicio de una empresa usuaria, debe tener un hardware y software óptimos para manejar los datagramas a la misma velocidad que la conexión, lo que se logra con un mecanismo de filtrado de alta velocidad conocido como filtrador de paquetes.[1]

El filtrador se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según nuestras indicaciones mediante un router con dos interfaces de red.

Existen también las pasarelas a nivel de aplicación que utilizan una puerta de acceso de uso obligatorio y tratan los servicios por separado, utilizando el código adecuado para cada uno. Atravesada la puerta esta determinará si da el servicio o establece la conexión con el ordenador que lo da.

Esta pasarela no necesita tratar complicadas listas de acceso y centraliza en un solo punto de gestión los servicios y son la solución efectiva para el tratamiento

[1] COMER (Douglas E.) Introducción al estudio del TCP/IP, Op.cit., p.489.

seguro de aquellos servicios que requieren permitir conexiones iniciadas desde el exterior (servicios como FTP, Telnet, Correo Electrónico).[1]

Por último tenemos las pasarelas a nivel de circuito, que se basan en el control del las conexiones TCP y actúan como un cable de red: por un lado reciben las peticiones de conexión a un puerto TCP; y por otro, establecen la conexión con el destinatario deseado, si se han cumplido las restricciones establecidas.

Este tipo de cortafuegos suelen trabajar conjuntamente con los servidores utilizados para la acreditación, es decir, comprobaciones sobre la máquina fuente, la máquina destino y el puerto a utilizar.

Estos muros de fuego son utilizados a la entrada del webserver para que autentique las direcciones IP, si no lo reconoce como un usuario autorizado no lo deja entrar, protegiendo toda la información que se encuentra detrás del muro.

[1] GONZALEZ T. (Patricio) VILLALÓN I. (Alvaro). Op.cit.

CAPÍTULO II:

LA CONTRATACIÓN ELECTRONICA

SECCION I: NOCIONES BÁSICAS DE TRANSMISIÓN DE INFORMACIÓN

Para iniciar el desarrollo del tema referente a la Contratación Electrónica es importante reconocer que el desarrollo de Internet es el que ha propiciado el desarrollo del Comercio Electrónico, teniendo ambas una relación directa; sin una no podría existir la otra.

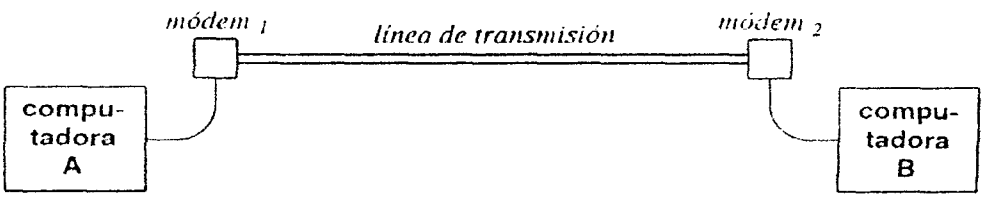
Es necesario además, tener una noción básica de cómo se transmite o "navega" la información en Internet para que de esa forma se pueda entender la dinámica del Comercio Electrónico.

En esta parte de la investigación se tratará de explicar de una manera clara y lo menos técnica posible los mecanismos de comunicación, siendo así más accesible a los estudiosos del Derecho.

a) COMUNICACIÓN BÁSICA ENTRE COMPUTADORAS

Las redes de computadoras conectan computadoras entre sí, de manera que puedan intercambiar información. Dichas redes son en la actualidad combinaciones complejas de hardware y software, muy alejadas de las redes de computadoras que se conocían al inicio.

Para que dos computadoras puedan comunicarse a través de Internet es necesario un modulador de un extremo y un demodulador en otro extremo; ese dispositivo de cada extremo se le conoce como módem (abreviatura de *mod*ulador/*dem*odulador) que comprende tanto al modulador que se usa para enviar información como el demodulador que se utiliza para recibir la información. [1]



Existen módems que permiten la comunicación por medio de conexiones telefónicas ordinarias, muchos permiten el envío de datos en ambas direcciones y cada módem contiene tanto un modulador como un demodulador.

"Un módem es un dispositivo necesario para la comunicación a través de una conexión telefónica ordinaria o para la comunicación a larga distancia por cable. Un módem soporta la comunicación en ambos sentidos, porque contiene un modulador para el envío de señales y un demodulador para su recepción" [2]

---

[1] COMER (Douglas E.). El libro de Internet, México, Editorial Prentice-Hall, Segunda Edición, 1.998, pág.32
[2] Ibid., pág.33

La accesibilidad a esta red obedece principalmente a que no fue diseñada para un conjunto específico de servicios, a diferencia de otras redes comerciales.

El solftware que proporciona los servicios de Internet ha sido construido en dos partes funcionales: 1) La primera contiene el software necesario que permite a las computadoras comunicarse y ésta puede utilizarse en cualquier servicio; y 2) La segunda, consiste en aplicaciones que proporcionan servicios de alto nivel.

Por ser los medios de comunicación de Internet de propósito general y eficiente, casi cualquier aplicación de red puede utilizar Internet.

Lo dicho anteriormente, justifica también el desarrollo tan masivo del Comercio Electrónico, por encontrarse al alcance de la mayoría de las personas que cuentan con una computadora.

Internet ofrece muchos servicios: se puede enviar correo electrónico o leer noticias, se puede obtener información sobre el tiempo, chistes, caricaturas, etc.

Los protocolos de Internet[1], por su parte proporciona los recursos básicos de comunicación utilizados en Internet, constituyéndose esos protocolos en la base de todos los servicios que presta esta red.

[1] Ver supra Protocolos de Internet, Título II, Capítulo I, Sección II

b) ¿CÓMO VIAJA LA INFORMACIÓN A TRAVES DE INTERNET?

Para entender cómo viaja la información a través de Internet debemos en primer lugar saber cuál información es la que viaja por ella.

Para distinguir entre paquetes enviados a través de Internet y paquetes de otras redes, los paquetes deben seguir el formato especificado por el Protocolo Internet, por lo que se les conoce el nombre de *datagramas IP*.

El nombre datagrama IP "fue escogido para dar una idea de cómo los maneja el servicio de entrega de paquetes de Internet. Como el nombre lo sugiere, Internet maneja datagramas de manera muy parecida a como una oficina de telégrafos maneja los telegramas: Una vez que la computadora transmisora crea un datagrama y éste comienza su viaje a través de Internet, el transmisor puede reanudar su procesamiento normal, de la misma forma que una persona puede seguir sus tareas después de enviar un telegrama. Un datagrama viaja a través de Internet de manera independiente del transmisor, igual que un telegrama viaja hacia su destino de manera independiente de la persona que lo envió."[1]

Desde el momento que la computadora tiene instalado el software IP, ya puede crear un datagrama IP y enviarlo a otra computadora. Esto porque el IP

---

[1] COMER (Douglas E.), El Libro de Internet, op.cit.,pág.108.

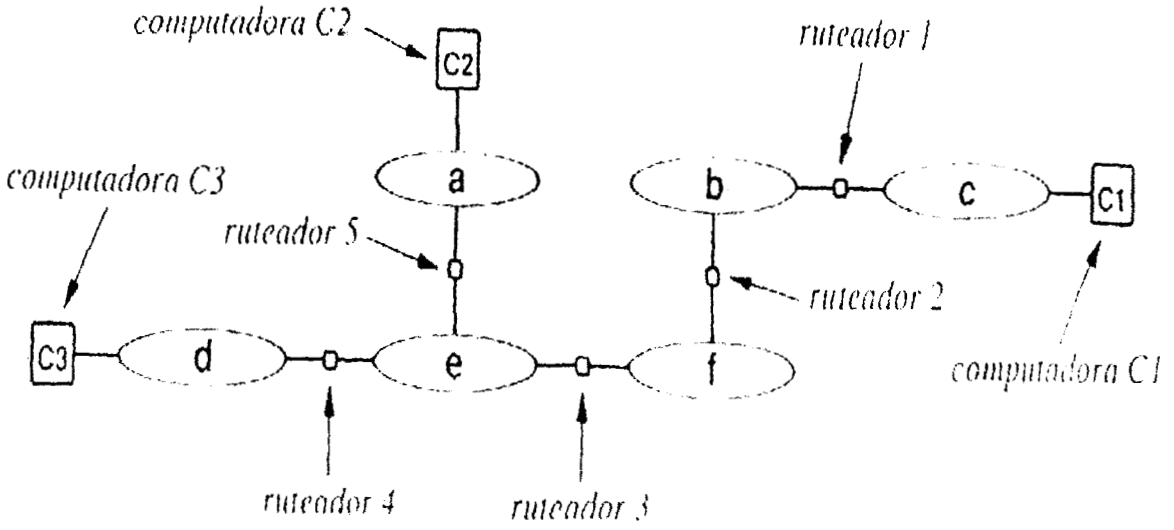
transforma un grupo de redes y ruteadores en un sistema intangible de comunicaciones, haciendo que Internet funcione como una sola y gran red.

Una vez que tenemos claro lo qué es un datagrama, nos parece oportuno ilustrar ahora cómo viajan esos datagramas por la red.

El escritor Douglas E. Comer ilustra claramente cómo trabaja el software IP (el que permite la transmisión de la información) de la siguiente forma:

"Imagínese que la computadora C1 se necesita comunicar con la C3. Para empezar, el software IP en C1 deber crear un datagrama IP. Cada datagrama tiene un campo que especifica la dirección IP del remitente y otro que especifica la dirección IP del destinatario. El datagrama que C1 crea contiene la dirección IP de C3 como destinatario y la dirección IP de C1 como remitente (u origen). Como dos computadoras no se conectan a la misma red, cualquier viaje de datagramas entre ellas debe pasar por un ruteador. C1 envía el datagrama a través de la red C al ruteador 1. El ruteador 1 examina la dirección de destino del datagrama C3, para determinar a dónde enviarlo. Como el destinatario se encuentra más allá de la red b, el ruteador 1 envía el datagrama a través de la red b al ruteador 2. El ruteador 2 examina la dirección de destino y envía el datagrama a través de la red f al ruteador 3. El ruteador 3 debe elegir entre el ruteador 4 y el 5. Este escoge enviar el datagrama a través de la red e al ruteador 4, debido a que dicho ruteador

conduce al destino final (el ruteador siempre escoge el camino más corto). El ruteador 4 percibe que puede entregar el datagrama a su destinatario final, C3, enviándolo a través de la red d. Si C3 le envía un datagrama de regreso a C1, dicho datagrama sigue el mismo camino en la dirección contraria." [1]



Por medio de Internet se brindan varios servicios como el correo electrónico, servicio de boletín electrónico, transferencia de archivos, acceso remoto (Telnet), servicios que son importantes par comerciar electrónicamente.

[1] COMER (Douglas E.) El Libro de Internet, op.cit., pág 113.

SECCIÓN II: COMERCIO ELECTRÓNICO

Tal y como se afirmó líneas atrás, la Contratación Electrónica se ha desarrollado conforme el desarrollo de Internet. La facilidad para accesar la red ha sido una razón importante para que los usuarios más comunes, sin importar los conocimientos que puedan tener en informática, puedan relacionarse directamente con la red.

Este fenómeno ha sido relevante para el Derecho ya que viene a cambiar en gran medida algunas nociones básicas tales como "comercio", "contrato", "medios de pago", "documento", etc.

Actualmente, nuestra economía y el Derecho se enfrentan a éstos cambios y a una serie de avances tecnológicos los cuales junto con las comunicaciones digitales han ido creando una economía sin fronteras.

El comercio ha sufrido una "desnaturalización", en el sentido de que no se realiza de la forma en la que se concibió antes de que la era informática dominara los mercados y existieran ya los cuerpos normativos que rigen la materia en específico.

La contratación electrónica ha ido transformando los procesos de producción, quedando la fabricación y el transporte del producto como los únicos actos realizados de la forma convencional.

En el comercio electrónico los actos jurídicos se realizan por medios electrónicos e informáticos dando origen al nacimiento de derechos y obligaciones personales y patrimoniales de una determinada forma y manera, los cuales son de interés para el Derecho con respecto a la regulación y control que debe tener sobre los mismos.

"Pero aunque los soportes, medios, formas y maneras "digitales" difieran de los habituales, el "contrato electrónico" es válido y existirá jurídicamente desde que una o varias personas consientan sin error, libre y voluntariamente, en obligarse entre ellas, a darse alguna cosa o prestarse algún servicio lícito y con causa. De este modo el concurso de la oferta y de la aceptación expresada por medios y sobre soportes electrónicos, o realizada con ayuda de programas o elaboradores electrónicos, perfeccionará el contrato electrónico."[1]

El escritor Barriuso parte de nociones básicas del Derecho y las traslada a la realidad "electrónica", aspecto que es acertado, ya que la actividad es la misma y lo

[1] BARRIUSO RUIZ (Carlos), La contratación electrónica, Madrid, Editorial Dykinson S.L., Primera Edición, 1.998, pág. 27.

único que cambia es el medio en que se realiza. No por eso debe dejar de ser un contrato; siempre y cuando cumpla con los requisitos que el Derecho reconoce en materia contractual, el acto jurídico se verificará como válido y eficaz, teniendo todos los efectos consecuentes.

En esta nueva actividad parece no darse un acuerdo en cuanto a la regulación que debe existir por desarrollarse en un campo nuevo para el Derecho y para el legislador, un campo no físico con individuos no determinados en cualquier lugar del mundo, lo que hace difícil el control de las actividades como el comercio electrónico, derechos de propiedad, etc.

El uso de estos nuevos medios trae consigo cambios fundamentales por ser nuevos agentes del comercio para las partes contratantes, que en algunos casos no existe siquiera la intervención humana.

a) CONCEPTO DE COMERCIO ELECTRÓNICO

En este apartado seleccionamos las definiciones que nos parecen más acertadas sobre lo qué es comercio electrónico.

El autor Renato Javier Jijena Leiva dice sobre el comercio electrónico lo siguiente: "Se ha definido como el intercambio telemático de información entre

personas que da lugar a una relación comercial, consistente en la entrega en línea de bienes intangibles o en un pedido electrónico de bienes tangibles." [1]

Por su parte el autor Carlos De Paladella señala en su concepto de comercio electrónico todas las actividades que pueden considerarse como tales: "El concepto de comercio electrónico no sólo incluye la compra y venta electrónica de bienes o servicios, que es el concepto común que se tiene, sino que también incorpora el uso de las redes para actividades anteriores o posteriores a la venta, como son: la publicidad, la búsqueda de información, el aseguramiento de las posibles transacciones, el tratamiento de clientes y proveedores, incluso inversores, trámites ante autoridades de control y fiscalización, la negociación de condiciones de compra, suministro, etc., la prestación de mantenimiento y servicios posventa y la colaboración entre empresas." [2]

En síntesis, el comercio electrónico consiste en realizar transacciones comerciales electrónicamente, entendiéndose "comerciales" en sentido amplio.

---

[1] JIJENA LEIVA (Renato Javier), Comercio Electrónico y Derecho. La problemática jurídica del Comercio Electrónico. Universidad Católica de Valparaíso, 1.999. Documento sin numeración, disponible en: HIPERVINCULO http://publicaciones. derecho.org/redi/

[2] DE PALADELLA (Carlos) citado por KNORR BRICEÑO (Jolene Marie) y ROLDAN SAUMA (Marcelo), La Protección del Consumidor en el Comercio Electrónico, Costa Rica, Editorial Investigaciones Jurídicas S.A., Primera Edición, 2.001, pág. 59.

b) ELEMENTOS DEL CONTRATO ELECTRÓNICO

La doctrina y la legislación en materia contractual han delineado los requisitos o elementos esenciales que deben darse en un contrato para que éste sea válido.

Los contratos electrónicos no crean una nueva teoría de las obligaciones, sino que conlleva a que los principios clásicos de la contratación deban ser revisados y actualizados a la luz de la nueva realidad tecnológica; esta realidad que rompe con la manera en que las partes convienen sus negocios.

El artículo número 1.008 del Código Civil vigente establece la necesidad de una manifestación libre y clara del consentimiento de las partes, lo que nos hace pensar que la identidad de las personas que contratan es muy importante tanto en la contratación tradicional como en la electrónica.

i- La identificación o identidad de las partes en el Contrato Electrónico.

"LA IDENTIDAD de las personas constituye la determinación de su personalidad a efectos de atribución de derechos y obligaciones" [1]

La identificación de las partes en un contrato nos permite exigir el cumplimiento a una persona determinada y de esta forma gozar de legitimidad

[1] BARRIUSO, RUIZ (Carlos) Op.cit, pág.49

tanto para la exigencia del cumplimiento como para impugnar su validez o ineficacia.

En la contratación tradicional (llamaremos así a la que no es electrónica), la identificación está compuesta por los nombres y apellidos propios de las personas, las partes pueden identificarse por medio de documentos como la cédula de identidad, el pasaporte, el permiso de conducir, etc., incluso podría utilizarse certificados, registros, títulos, partidas, actas notariales, etc. La identificación como medio para determinar la identidad de las personas se verifica por medio de la firma y también por signos como las huellas digitales.

En la contratación electrónica, evidentemente estos medios de identificación no son posibles de utilizar porque el medio no lo permite del todo, por eso se debió crear formas de identificación. Entre las formas de identificación en la contratación electrónica tenemos el uso de códigos, claves, login, passwords, passphrase, la firma electrónica, la firma gráfica digital y tarjetas electrónicas con banda magnética o con chip incorporado (inteligentes) elementos que permiten individualizar a las partes.

"Por cuestiones de seguridad y confidencialidad debido a la forma en que se transmite la información en las actuales redes de comunicación, se aconseja un tratamiento criptográfico de los datos de identificación y residencia."[1]

La firma digital electrónica (que desarrollaremos ampliamente más adelante) tiene los mismos fines que la manuscrita, pero además manifiesta identidad y la autoría, la autentificación, la integridad, la fecha, la hora y recepción, a través de métodos criptográficos asimétricos de clave pública (RSA, GAMAL, PGP, DSA,LUC, etc.), técnicas de sellamiento electrónico y funciones de Hash, lo que hace que la firma esté en función del documento que se suscribe, que la hace absolutamente inimitable como no se tenga la clave privada con la que está encriptada, verdadera atribución de la identidad y autoría.

La identificación es importante, ya que por medio de ella podemos determinar la autoría de la declaración de voluntad y autentificar el contenido, siendo las mismas personales e intransferibles.

En la contratación electrónica es necesario además identificar los instrumentos interpuestos de hardware y software, para los ordenadores se determina a través de los nombres DNS o números IP, la dirección de correo electrónico, la clave de acceso a los Host identificados, para el resto se debe

[1] BARRIUSO RUIZ (Carlos) Op.cit, pág. 50

siempre tomar constancia de las características técnicas, físicas y lógicas del sistema de contratación electrónica así como los soportes informáticos y electrónicos, lo que nos ayudará en caso de tener que investigar el documento.

Todas las herramientas que la informática nos proporciona serán de gran ayuda para saber si la persona que contrata es quien dice ser, que es capaz para realizar contratos y que las manifestaciones son hechas por él.

Dentro de las herramientas que nos pueden ayudar a esa tarea tenemos las entidades de certificación de claves, técnicas criptográficas, identificación magnética y las "NOTARÍAS ELECTRÓNICAS", éstas últimas parte del eje central de nuestra investigación y las cuales desarrollaremos ampliamente más adelante.

Tenemos que ser concientes que si cedemos nuestras claves estaríamos cediendo practicamente nuestra identidad, por lo tanto si el titular de la clave es negligente con su uso, éste será responsable de todas las consecuencias.

El tema de la identificación es crucial si tomamos en cuenta que al no existir una relación física entre las partes, por realizarse el negocio a distancia, sin domicilios convencionales y sin documentos materializados en papel, queda

únicamente para su validez las claves, códigos e información digital suministrada, siendo necesario entonces una Notaría Electrónica.

ii- Capacidad de las partes en el Contrato Electrónico.

En lo referente al tema de la capacidad hay que distinguir entre capacidad jurídica y capacidad de actuar.

El artículo 36 del Código Civil establece que: "la capacidad jurídica es inherente a las personas durante su existencia, de un modo absoluto y general. Respecto de las personas físicas, se modifica o se limita según la ley, por su estado civil, su capacida volitiva o cognocitiva o su incapacidad legal; en las personas jurídicas por la ley que las regula."[1]

El artículo citado supra, define claramente qué es la capacidad jurídica (es inherente a las personas durante su existencia de modo absoluto y general), quiere decir que desde el nacimiento todas las personas sin importar edad, estado civil, capacidad volitiva, etc., tienen dicha capacidad. Por su parte la capacidad de actuar sólo la tienen, por decirlo de alguna forma, las personas que cumplen con ciertos requisitos. Por eso nos parece que dicho artículo confunde la capacidad

[1] Código Civil, artículo 36.

jurídica con la capacidad de actuar al no ser del todo claro en su redacción. Para nuestros efectos, nos interesa únicamente la capacidad de actuar.

En lo que se refiere a la edad, nuestro Código considera que son mayores las personas que han cumplido dieciocho años y menores los que no han llegado a esa edad. Se ha expresado que la mayoridad señala la época a partir de la cual la persona es considerada con la necesaria capacidad para el ejercicio directo de la contratación y demás actos de la vida civil.

También realiza nuestro Derecho Civil una bipartición de la minoridad, poniendo como edad que divide la vida del menor la de quince años. El menor de quince años es persona absolutamente incapaz para obligarse por actos o contratos que personalmente ejecute o celebre salvo lo dispuesto sobre el matrimonio. En cuanto al mayor de quince años pero menor de dieciocho, si bien sus actos en general están viciados por no gozar aún de la plenitud de su capacidad, el vicio del que adolecen implica sólo nulidad relativa de tal forma que pueden convalidarse por él expresa o tácitamente una vez que entre en la mayoridad.

Respecto a la capacidad mental, los actos o contratos que realice una persona que adolece de esta capacidad serán absolutamente nulos si al celebrarlos estuviere declarada la incapacidad por sentencia inscrita en el correspondiente registro, son, sin embargo, relativamente nulos cuando no tiene lugar esta hipótesis. El artículo

41 del Código Civil establece que "los actos o contratos que se realicen sin capacidad volitiva y cognocitiva serán relativamente nulos, salvo que la incapacidad esté declarada judicialmente, en cuyo caso serán absolutamente nulos."[1]

En el comercio electrónico, no sólo tiene que estar identificadas las partes, hay además que determinar si ostentan la capacidad legal de obrar y de contratar. En la contratación electrónica es especialmente difícil de comprobar ya que no hay una apreciación directa entre las partes por el elemento "distancia". "No obstante, las últimas tecnologías permiten tener en pantalla la imagen, la voz e incluso la escritura en directo de la otra parte, lo que minimiza en cierto modo el problema."[2]

En la contratación electrónica las prohibiciones e incapacidades deben constatarse de alguna forma para salvaguardar en todos los aspectos al contrato, ya que la falta de capacidad hace ineficaz el consentimiento, requisito esencial para la validez de los contratos.

"Lo usual es que antes del momento de la contratación electrónica se lleven a cabo actos de comprobación de esta capacidad, con preacuerdos. Pero también debería ser comprobado en el momento de contratar el acceso a la red (Internet)

---

[1] Código Civil, artículo 41.
[2] BARRIUSO RUIZ (Carlos), op.cit, pág.66

por el centro proveedor, al suscribir el contrato de prestación de servicios "on line" con el usuario. Así, la única forma de contratar sería usando ilegítimamente claves pertenecientes a otros. En caso contrario, hasta el propio contrato de acceso quedaría afectado."[1]

iii- La representación de las partes en el Contrato Electrónico.

La representación es conocida por nuestra legislación bajo la figura jurídica del contrato de mandato y se hace constar mediante el instrumento llamado "poder".

Por medio de los poderes, dependiendo del tipo que se trate, el apoderado puede actuar legalmente en representación de su mandante y sus actuaciones se reputarán como realizadas por éste último.

El Código Civil en su artículo 1.252 establece que: "el contrato de mandato se reputa perfecto por la aceptación tácita o expresa del apoderado o mandatario. La aceptación tácita se presume por cualquier acto en ejecución del mandato; excepto los que se hicieren para evitar perjuicios al mandante mientras nombra otro apoderado."[2]

---

[1] BARRIUSO RUIZ (Carlos) Op.cit, pág .67
[2] Código Civil, artículo 1.252

En la contratación electrónica es difícil determinar la naturaleza de la representación con que se actúa.

"En la representación, el representante sustituye al representado, y sus manifestaciones de voluntad, obligan al representado que se convierte en titular del derecho en la relación negocial concertada por el representante."[1]

La representación en la contratación electrónica puede darse de tres formas:

a) contratación realizada por un representante sin que nunca se la hubiese apoderado para ese acto;

b) con poder revocado o vencido; y

c) con poder.

a) Contratación realizada por un representante sin que nunca se le hubiese apoderado para ese acto:

En este caso concreto, los contratos celebrados a nombre de otro por una persona que no goza la representación legal se reputará como nulo, al menos de que lo ratifique la persona a cuyo nombre se actuó antes de que éste el contrato sea revocado por la otra parte.

El actuar de esta forma puede traer consigo consecuencias tales como, la inexistencia del contrato, si la otra parte contratante lo revoca antes de la

[1] BARRIUSO RUIZ (Carlos) , op.cit, pág.68

ratificación, o si hubiera fallecimiento o incapacidad sobrevenida de cualquiera de los contratantes sin haber sido ratificado; validez del contrato si es ratificado, prestando consentimiento a posteriori y con efectos retroactivos.

b) Contratación efectuada por un representante con poder revocado o vencido:

En estos casos es necesario que la persona titular en cuyo nombre se actuó, haya comunicado la revocación de poder a la otra parte, si omite dicha comunicación será responsable de todo lo actuado.

Además las partes contractuales deben verificar la vigencia de los poderes de las personas con que contratan, para que se actúe con poderes vencidos.

c) Contratación efectuada por un representante con poder:

Este tipo de poder le otorga a los actos la misma eficacia al contrato como si hubiera sido realizado por el mandante. Es necesario que este poder sea acreditado por medio de claves para el representante y así determinar claramente la contratación. Es conveniente por eso, utilizar una clave distinta para el apoderado y otra para el mandante, de esta forma se podrá saber cuándo es que está actuando cada uno de ellos. Esto permitiría determinar los casos de abuso del poder.

"Los elementos de reconocimiento biométrico u otros semejantes acoplados a algún puerto del ordenador, obviarían el problema y se obtendría la mayor

certeza (en algunos casos irrefutable), en la determinación e identificación del contratante o del usuario. También los centros de compensación o notarías electrónicas, pueden controlar la representación mediante acreditación fehaciente, acabando así con la inseguridad de otros métodos."[1]

Podemos ver que en realidad es viable la obtención de medios que permitan reconocer en la contratación electrónica la forma en que se está actuando. Si se puede reconocer eso, se podría empezar a determinar responsabilidades por actuaciones fraudulentas, siempre y cuando se haga uso responsable de los passwords y claves que se otorguen.

iv- El Consentimiento de las partes en el Contrato Electrónico.

No cabe la menor duda de que este elemento es sumamente importante en materia de contratación ya que se podría decir que es el "cierre" del mismo, pueden las partes ponerse de acuerdo, redactar documentos relacionados, etc., pero si no expresan su consentimiento, el contrato no se concreta definitivamente. Nuestro Código Civil determina cómo debe ser el consentimiento de las partes en la contratación. El artículo 1.008 dice que "el consentimiento de las partes debe ser

[1] BARRIUSO RUIZ (Carlos), op.cit, pág. 72

libre y claramente manifestado. La manifestación puede ser hecha de palabra, por escrito o por hechos de que necesariamente se deduzca."[1]

Los contratos que presentan algún error en el consentimiento son anulables; así lo establece nuestra normativa al respecto. Los artículos 1.015 y 1.017 respectivamente, establecen cuáles casos son anulables, como por ejemplo cuando se consiente por error y ese error recae sobre la especiae de acto o contrato que se celebra o cuando recae sobre la identidad de la cosa específica de que se trata, o sobre su sustancia o calidad esencial; son anulables también los contratos que se suscribieron mediando la fuerza o el miedo grave. La fuerza y la intimidación también pueden viciar el consentimiento, y éstas no necesariamente tienen que llevarlas a cabo el beneficiado, puede ser cualquier tercero el que haya forzado con el objeto de obtener el consentimiento. [2]

El dolo por su parte no vicia el consentimiento, sino cuando es obra de una de las partes y cuando además aparece claramente que sin él no hubiere habido contrato. En los demás casos el dolo da lugar solamente a la acción de daños y perjuicios contra la persona que lo han fraguado o se han aprovechado de él;

[1] Código civil, artículo 1.008
[2] Código Civil, artículos 1.015 y 1.0017.

contra los primeros por el valor total de los perjuicios, y contra los segundos hasta el monto del provecho reportado.[1]

La contratación electrónica es una nueva forma de expresar, transmitir y manifestar la voluntad. En la contratación tradicional, hecha en papel y con firma autógrafa, la declaración de la voluntad se refleja normalmente, en la contratación electrónica, hecha en forma digital, con firma digital, pago electrónico, etc., la declaración de la voluntad se refleja por partes o en distintos actos.

El consentimiento electrónico constituye una modalidad especial de la declaración de voluntad negocial.

El consentimiento otorgado a derecho debe ser expresado con la declaración y acuerdo libre y consiente de voluntades que recae sobre la cosa y la causa en la contratación electrónica.

Por lo tanto, el consentimiento otorgado por medios electrónicos es válido, siendo necesario solamente el hecho que sea terminante, claro e inequívoco, consagrándose de este modo el principio de *autonomía de la voluntad* y el de *libertad contractual*, limitándose únicamente a las normas imperativas, de orden público, moral, buena fe, utilidad pública e interés social.

[1] Código Civil, artículo 1.020.

La voluntad generadora del consentimiento para ser válida tiene que ser consiente y libre, lo cual sólo puede hacerlo las personas humanas, además, el contrato existe desde que una o varias personas consientan en obligarse, siendo éstas últimas las únicas generadoras de voluntad para la existencia del contrato.

Por tratarse de comercio electrónico, la declaración de la voluntad o el consentimiento se expresa de una forma distinta a la usual, por eso "nuestro acto de voluntad determinante es la activación del sistema, que se completa con la voluntad ya expresada y subyacente en el programa. Pero si el sistema tuviere que encontrar coordenadas o parámetros prefijados para la realización de la contratación y no los encontrase, el contrato no se llevaría a efecto."[1]

El consentimiento por este medio se da activando medios electrónicos o mediante un sistema experto de ayuda a la decisión, entonces desde que el contratante da por bueno el sistema y lo activa, convalida cualquier proceso del sistema que actúe fiel a su programación y sin errores.

Cuando afirmamos que el consentimiento en la contratación electrónica se da por medio de varias facetas es porque el consentimiento está compuesto por: "motivación, intención, deliberación, decisión, expresión o manifestación, transmisión y conocimiento o toma de razón, por el oferente, habrá que examinar

[1] BARRIUSO RUIZ (Carlos) Op.cit., pág. 98

cada programa o cada contratación electrónica para determinar el grado de instrumentalización y de reflejo de voluntad diferida o potencial."[1]

Por vía electrónica, el consentimiento se determinará por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato.

No debe existir duda de la validez del contrato electrónico, pues existe contrato desde que las partes consienten en obligarse. Esa declaración pura del consentimiento, sea electrónico o tradicional, descansa en los mismos principios generales de libertad de expresión, autonomía de la voluntad y libertad de contratación. [2]

No debemos confundir manifestación de voluntad y la forma de dicha manifestación, que son importantes en los contratos denominados "solemnes". La forma no es expresión necesaria del negocio, sino un elemento instrumental que se añade al consentimiento y que tiene que ver con su prueba y no con la perfección del contrato, por lo que en principio cualquier contrato en que la ley no exige la forma escrita, podrá ser realizado electrónicamente.

---

[1] BARRIUSO RUIZ (Carlos) Op.cit., pág. 96.
[2] MATEU DE ROS (Rafael) El consentimiento y el Proceso de Contratación Electrónica. Derecho de Internet. Contratación electrónica y firma digital, España, Editorial Aranzadi S.A., 1° Edición, 2000, p. 30

CAPÍTULO III

FORMACIÓN DEL CONTRATO ELECTRÓNICO

SECCION I: REGULACIÓN Y VALIDEZ DE LOS CONTRATOS ELECTRÓNICOS

Los principios y bases del Derecho Común son perfectamente válidos en materia de contratación electrónica, cuando no existe una legislación específica como es el caso de Costa Rica.

Países como España, que actualmente tienen toda una legislación del tema, se iniciaron aplicando las reglas del derecho común y las fueron adaptando a las necesidades y realidades del nuevo medio de contratación.

Los contratos electrónicos tienen características propias, esto es lógico si pensamos que a pesar de estudiarse partiendo de principios de Derecho ya conocidos, el medio por el que se perfecciona es muy distinto al de los contratos usuales teniendo características propias.

Algunas características más representativas del contrato electrónico son las siguientes:

1- La desmaterialización del documento electrónico.

2- La esencialidad de los mensajes, por la existencia de acuerdos previos o de configuraciones explícitas.

3- La incorporeidad de las relaciones, por llevarse a cabo sin la presencia física de las partes.

4- La aparición de transferencias y flujos de datos electrónicos, que en la mayoría de los casos tienen efectos internacionales.

5- Las distintas fases de formación del consentimiento.

De esta forma, el contrato electrónico adquiere reconocimiento jurídico, ya que tiene las características de los contratos tradicionales. Así vemos que la firma digital equivale y sustituye a la firma autógrafa; el soporte del documento con los programas informáticos que hacen posible la determinación de la integridad, autoría y autenticación del contenido; etc.

En realidad, se hace necesaria la creación de una normativa internacional específica que logre regular homogéneamente la materia contractual electrónica, pues por el momento lo que se crean son regulaciones muy generales y sectoriales, como por ejemplo en nuestro país con la regulación de la firma digital que facilitará el comercio electrónico.

Nos encontramos frente a una preocupación general en busca de una legislación armónica. Estudios realizados sobre el comercio electrónico dejan latente esa necesidad, tal es el caso del escritor Carlos Barriuso Ruiz, que al respecto expresa: "Los acuerdos de voluntades reflejados a través de dispositivos electrónicos, informáticos o telemáticos establecen un nuevo marco jurídico de relaciones jurídicas, constitutivo de derechos y obligaciones, que cada día aumenta

exponencialmente y demanda su regulación específica en nuestro ordenamiento, en armonía con la de otros estados..."[1]

La doctrina ha establecido formas contractuales, las cuales determinan los efectos que los contratos deben tener, como las: **a)** *"ad solemnitatem"* que exigen para su validez la forma (por ejemplo, que sea otorgado en escritura pública), y **b)** *"ad probationem"* si lo que se quiere es beneficiarse de la prueba que ellos constituyen. Nuestro Código Civil, en el artículo 1.007 establece que: "además de las condiciones indispensables para la validez de las obligaciones en general, para las que nacen de contrato se requiere el consentimiento y que se cumplan las *solemnidades* que la ley exija."[2]

Tenemos entonces que si la ley exige *la forma* para darle valor al contrato, la desmaterialización del documento en la contratación electrónica sería un impedimento para cumplir con ese requisito. Pero si el contrato electrónico se valora por su ritual y procedimientos, debe aceptarse su existencia.

Por lo anterior, es que se estudia la posibilidad de que se pueda realizar la inscripción en los Registros Públicos de los documentos notariales electrónicos, ya que estas limitaciones "ad solemnitatem" serían prácticamente imposibles de

---

[1] BARRIUSO RUIZ (Carlos) Op.cit, pág. 79
[2] Código Civil, artículo número 1.007

resolver y se convierten en un verdadero problema para la contratación electrónica.

Por eso es que por medio de esta investigación se propone el establecimiento de notarías electrónicas con aplicación de técnicas de autoría y autentificación, en la que interviene un notario público y con la posibilidad de inscribir en el Registro los documentos electrónicos, cumpliéndose de esta forma con las formalidades contractuales (sobre este tema se desarrollará ampliamente más adelante).

Como el contrato electrónico se basa estrictamente en principios de derecho común, en la formación de estos se da el principio de la autonomía de la voluntad. Este principio permite a las partes establecer los pactos, cláusulas y condiciones que crean convenientes, siempre y cuando no sean contrarios a la ley, la moral y el orden público. Además establece la obligación de cumplimiento de lo pactado, vinculando a las partes contratantes que deben adaptar su conducta a lo pactado.

Esto se puede ir infiriendo de los principios generales, pero siempre será necesario ir normando las actividades que requieren contratos específicos.

Con el desarrollo de una legislación de contratación electrónica, se avanzaría en temas que ya en Europa se está trabajando desde los años 90, como por ejemplo, existe una propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la comercialización a distancia de servicios financieros

destinados a los consumidores, en que se determinan los derechos y obligaciones de las partes en la contratación, el derecho de retractación, el pago de los servicios antes de la retractación, la carga de la prueba del incumplimiento de obligaciones de proveedores y el consentimiento del consumidor.[1]

SECCIÓN II: FASES DE LA CONTRATACIÓN ELECTRÓNICA

El contrato electrónico goza de distintas fases que coadyuvan a la formación de la voluntad en diferentes momentos. En este punto de nuestra investigación ya podemos identificar algunas de ellas.

a) Fases iniciales, en ellas aún no hay obligación de contratar, es donde se confecciona la plataforma de actuación y se establecen las claves, códigos y sistemas para que validen las operaciones, pasando por los momentos de creación o aceptación del programa, sistema experto o software de ayuda a la decisión, en mayor o menor medida se patentizan las fases de nuestra voluntad negocial.

b) Fases decisivas, en ellas las partes contratantes inician la activación del sistema, que terminará en el momento de la declaración, en el encuentro de parámetros prefijados, con la fase de transmisión

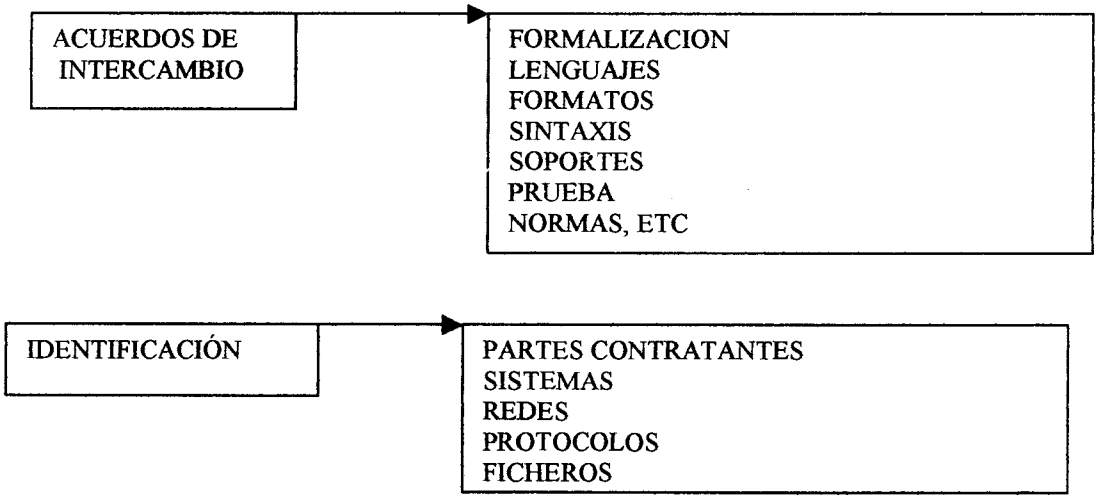
[1] Propuesta de Directiva del Parlamento Europeo y del Consejo 98/0245, del 19 de Noviembre de 1998.

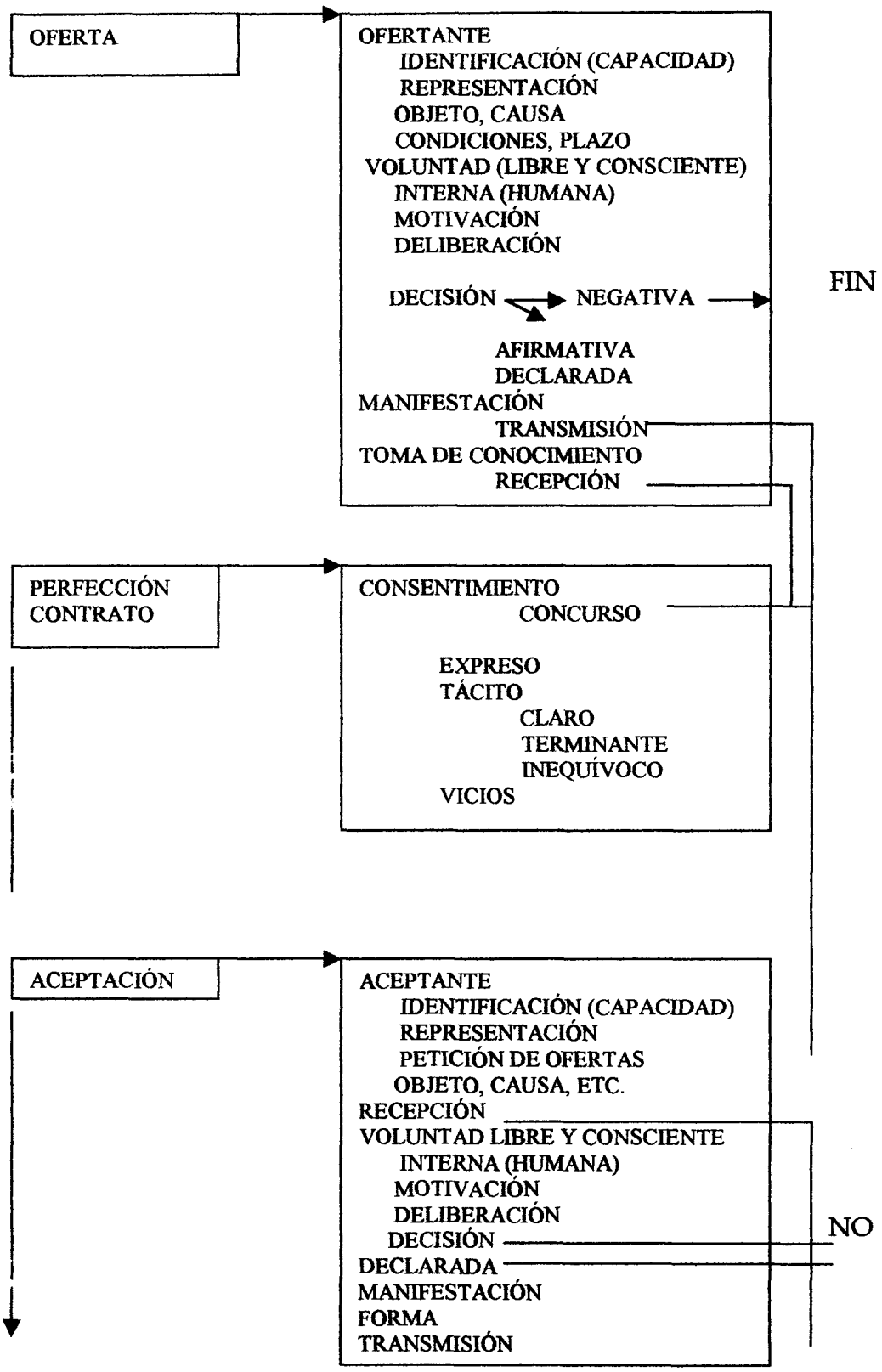
electrónica de la declaración de voluntad y la toma de razón de la aceptación del oferente. El cumplimiento mediante dinero electrónico y la entrega del producto cuando sea de naturaleza binaria, finalizarán las fases del contrato electrónico.

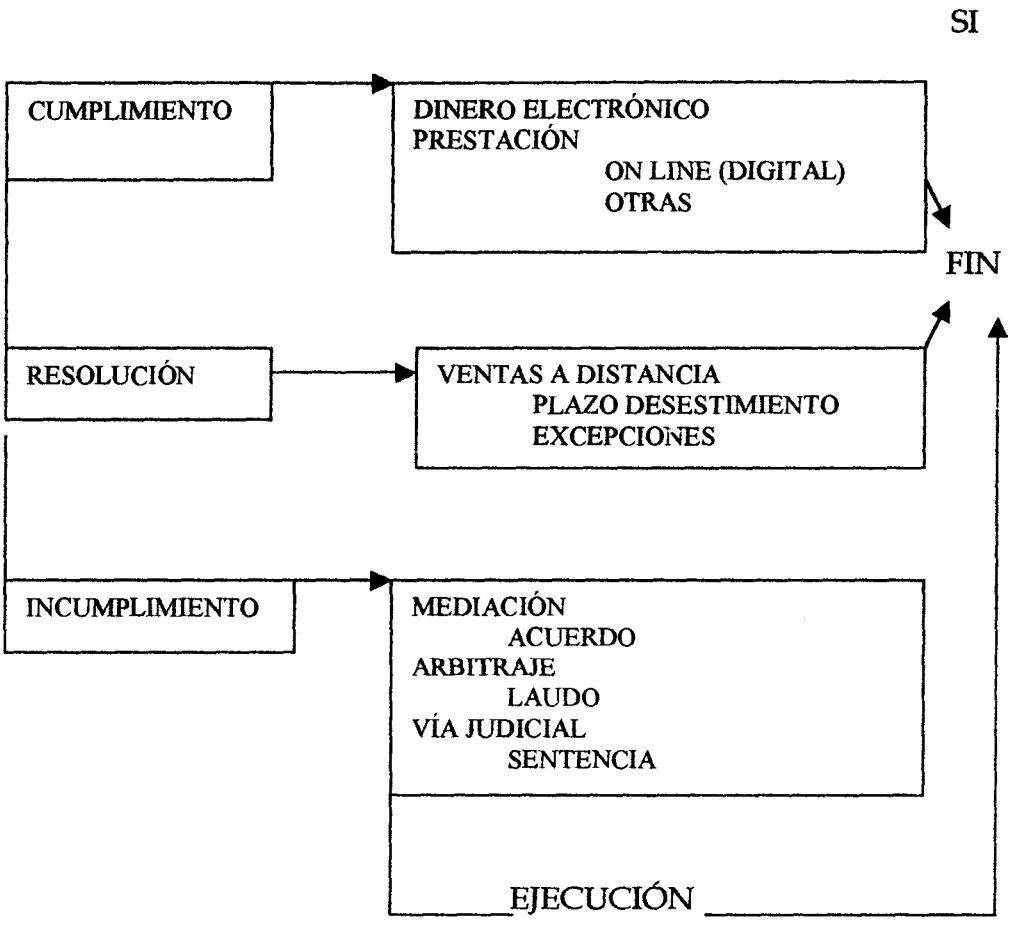
A continuación trataremos de esquematizar las fases de la formación de la voluntad y su reflejo en la contratación electrónica.

Para esos efectos y por parecernos sumamente claro utilizaremos un cuadro elaborado por el profesor Carlos Barriuso Ruiz, que nos ayudará a asimilar el concepto y la dinámica de la contratación electrónica.

FASES DEL CONTRATO ELECTRÓNICO




OFERTA
OFERTANTE
IDENTIFICACIÓN (CAPACIDAD)
REPRESENTACIÓN
OBJETO, CAUSA
CONDICIONES, PLAZO
VOLUNTAD (LIBRE Y CONSCIENTE)
INTERNA (HUMANA)
MOTIVACIÓN
DELIBERACIÓN
DECISIÓN
NEGATIVA
FIN
AFIRMATIVA
DECLARADA
MANIFESTACIÓN
TRANSMISIÓN
TOMA DE CONOCIMIENTO
RECEPCIÓN
PERFECCIÓN CONTRATO
CONSENTIMIENTO
CONCURSO
EXPRESO
TÁCITO
CLARO
TERMINANTE
INEQUÍVOCO
VICIOS
ACEPTACIÓN
ACEPTANTE
IDENTIFICACIÓN (CAPACIDAD)
REPRESENTACIÓN
PETICIÓN DE OFERTAS
OBJETO, CAUSA, ETC.
RECEPCIÓN
VOLUNTAD LIBRE Y CONSCIENTE
INTERNA (HUMANA)
MOTIVACIÓN
DELIBERACIÓN
DECISIÓN
NO
DECLARADA
MANIFESTACIÓN
FORMA
TRANSMISIÓN



En la contratación electrónica, las partes pueden elaborar un borrador del contrato con cualquier procesador de texto, encriptarlo con el software apropiado y enviarlo al destinatario, quien lo desencriptará y hará las correcciones que crea convenientes, lo devuelve y una vez que se haya establecido el texto definitivo, se firmaría electrónicamente, momento en que se perfeccionará el contrato.

Como podemos ver, se afirma una vez más la necesidad de que el consentimiento sea completamente expreso, terminante, claro, inequívoco para que sea válido, si éste es válido hará que el contrato lo sea, siempre y cuando concurran también el objeto cierto y la causa de la obligación.

Para que se dé el perfeccionamiento del contrato electrónico, el ánimo tiene que ser expresado por medios y sobre soportes electrónicos, o con la ayuda de programas o elaboradores electrónicos, siempre que se cumplan con las condiciones esenciales para la validez de los contratos. La oferta hecha electrónicamente es válida y el contrato se perfeccionará con la sola aceptación, siendo como único requisito para ésta que sea clara e inequívoca, sin importar la forma.

Respecto al lugar y momento de la formación del contrato nos tenemos que ubicar en los supuestos de la relación contractual entre ausentes.

"La formación del contrato, determina el lugar y el momento de nacimiento de la obligación y las consecuencias jurídicas que ello conlleva, ya que puede determinar la competencia territorial de los tribunales que deban conocer de estos asuntos o contratos y la ley nacional aplicable a cada caso, acto o contrato. El momento de su formación, entendemos es el de la recepción de la oferta, en el momento y en el lugar en que el oferente recibe la aceptación de la oferta;

siguiendo la teoría "civilista" de la cognición, que lo entiende concluido cuando el ofertante conoce la aceptación de su oferta." [1] En este caso puede ser la llegada al buzón del ofertante.

El lugar de celebración será donde se hizo la oferta, siendo lo habitual en contratación electrónica el sometimiento de las partes a un proceso de arbitraje. Con las nuevas tecnologías que se nos presentan, es muy probable que se pueda contratar desde un avión, ferrocarril, buque incluso automóvil quedando regidos a la ley del lugar de abanderamiento, registro, matrícula y si es en carretera sería del lugar donde se hallen.

El objeto de la obligación contractual electrónica es la prestación y pueden ser objeto del contrato todas las cosas que no están fuera del comercio de los hombres, tiene un tratamiento exactamente igual que las contrataciones tradicionales, en las que se puede ser objeto del contrato además todas las cosas que no estén fuera del comercio de los hombres, que no sean contrarias a la ley o a las buenas costumbres, que sean posibles y determinadas en su especie; y la cantidad se pueda determinar sin que sea necesario un nuevo convenio. Es posible la existencia de un contrato en el que el objeto del mismo no exista antes ni durante la celebración del mismo, tratándose de una cosa futura.

---

[1] BARRIUSO RUIZ (Carlos) Op.cit, pág. 133

La causa es la finalidad que se pretende con la contratación y por tanto debe existir, ser licita y cierta, por lo que los contratos sin causa o con causa ilícita o los que se opongan a las leyes o la moral no producen ningún efecto. La falta de ésta no puede ser subsanable ya que debe existir antes del contrato y se presume lícita salvo prueba en contrario. Corresponde a los tribunales la apreciación de la existencia o no de los requisitos del contrato como la causa por ejemplo.

El contrato electrónico debe incluir ciertas cláusulas generales tales como: la fecha, lugar de celebración, identificación de las partes contratantes, calidad de su intervención, capacidad, domicilio social, web y dirección de e-mail, oferta, productos o servicios, consentimiento, forma de manifestarlo, aceptación libre y voluntaria, idioma, registro, impuestos, etc. Además de las cláusulas que necesarias como: Objetivos, Condiciones Técnicas, Indemnizaciones, Modificaciones, Responsabilidad, Mantenimiento, Entire Agreement (implica el haber leído y entendido el contrato, con exclusión de cualquier otro pacto o cláusula anterior a la fecha del contrato), Propiedad intelectual e industrial, Confidencialidad, Exclusividad, Garantía, Fuero, Cumplimiento, Plazo, Resolución, Precio, Firma, Acuerdo marco.

SECCIÓN III: MEDIOS ELECTRÓNICOS DE PAGO

Para el Derecho, el dinero es un signo convencional de valor, con la consideración de un mueble fungible, que se utiliza como medio de intercambio y pago, cuya representación oficializa el Estado a través de sus autoridades monetarias. El dinero funcional como instrumento de intercambio económico.

Es obvio que las transacciones realizadas por medios electrónicos, como por ejemplo, una compraventa, necesitan para su perfeccionamiento que se verifique un pago.

Los pagos de las transacciones electrónicas se realizan también por un medio electrónico que sería: "cualquier transferencia de fondos, distinta a una transacción generada por un cheque, una letra de cambio o un instrumento de pago de papel, la cual se inicia a través de un terminal electrónico, instrumento telefónico o un computador o una cinta magnética a fin de ordenar, dar instrucciones, o autoriza a una Institución Financiera para que adeude o acepte pagos en una cuenta. Dicho término incluye, pero no está limitado a las transferencias originadas, los puntos de ventas electrónicos, las transacciones de los cajeros automáticos, los depósitos directos o los reintegros de fondos, y las transferencias originadas por telefonía."[1]

[1] BARRIUSO RUIZ (Carlos) Op.cit, pág 272

Estos nuevos medios de pago son avances tecnológicos que facilitan el comercio electrónico. Son semejantes a los medios de pago tradicionales como el dinero en efectivo, el cheque, la tarjeta de crédito y las tarjetas de débito. Mencionaremos algunos de los medios electrónicos de pago mas utilizados y sus rasgos más característicos:

a) Dinero Electrónico:

Es más conocido como "Monedero electrónico". Por este medio el usuario se conecta en línea con su banco o con un tercero (compañía intermediaria) y retira una cantidad de monedas electrónicas de su cuenta que guarda en el disco duro de su computadora, en una especie de "monedero electrónico" introducido a la computadora del usuario por un software (generalmente denominado Wallet).

El usuario podrá utilizar este dinero a su gusto y realizar pagos a vendedores o individuos que acepten este tipo de transacción. "Las ventajas de este sistema consisten en que los datos de tipo económico del consumidor no circulan constantemente por la Red, permitiendo así una mayor seguridad y privacidad sobre sus datos personales."[1]

[1] KNORR BRICEÑO (Jolene Marie) y ROLDAN SAUMA (Marcelo) Op.cit, pág.51

b) El Cheque Electrónico.

Es considerado como uno de los medios de pago más seguros con los que cuentan hoy día los Bancos. Se utilizan técnicas de autenticación, firma digital, certificados por autoridad competente y encriptación.

No son muy diferentes a los cheques comunes, pues contienen los mismos datos y se basan en el mismo sistema legal. Pueden contener todo tipo de información e intercambiarse directamente entre las partes. "Su funcionamiento se desarrolla de la siguiente manera: en primer lugar, el consumidor escribe el cheque utilizando un procesador de texto y lo remite al pagador también mediante medios electrónicos. A continuación, el pagador deposita el cheque electrónico en un banco y recibe crédito. El banco que recepciona el cheque electrónico lo convalida con el banco emisor, lo acredita directamente en la cuenta de este último."[1]

En realidad, el cheque electrónico lo que hace es autorizar el traslado de dinero de una cuenta bancaria a otra, contando con la firma digital.

c) Tarjeta Mondex.

Se trata de una tarjeta inteligente muy parecida a las tarjetas telefónicas; tienen un chip muy pequeño que funciona como una memoria. En él se

[1]KNORR BRICEÑO (Jolene Marie) y ROLDAN SAUMA (Marcelo) Op.cit, pág. 52

almacenan tanto el dinero que se quiere llevar en el bolsillo, como los programas de seguridad que protegen su contenido, haciendo muy seguras las transacciones.

"La ventaja que ofrece es que el dinero se transfiere directamente al vendedor cuando se retira el producto adquirido, sin tener que acudir a una transacción en línea o una incómoda operación de verificación y autenticación."[1]

d) La Tarjeta de Crédito.

Existe mucho temor respecto al uso de la tarjeta de crédito como medio de pago electrónico, ya que carece de un software de encriptación especializado. Los números de la tarjeta de crédito se transmiten sin estar cifrados, por lo que este tipo de información podría ser interceptada por "crackers" (se dedican a romper los sistemas de seguridad e ingresar a bases de datos de instituciones y bancos).

En Costa Rica, uno de los principales obstáculos para el desarrollo del comercio electrónico ha sido la oposición de las compañías de tarjetas de crédito para aceptar las transacciones electrónicas, pues en ellas no se recoge la firma del cliente por escrito. Según coinciden algunos expertos, esto ha provocado que en

[1]KNORR BRICEÑO (Jolene Marie) y ROLDAN SAUMA (Marcelo) Op.cit, pág. 53

muchos sitios sólo acepten pagos en efectivo, y que en otros se haya buscado establecer convenios con empresas de este tipo en el extranjero."[1]

Estos medios de pago son los más conocidos y utilizados, los cuales tienen características comunes por medio de las cuales se pueden identificar las consecuencias jurídicas que su uso pueda traer.

[1]KNORR BRICEÑO (Jolene Marie) y ROLDAN SAUMA (Marcelo) Op.cit, pág. 54

TITULO TERCERO

LA FUNCIÓN NOTARIAL ELECTRÓNICA

CAPÍTULO PRIMERO

EL DOCUMENTO ELECTRÓNICO

SECCION I: CONCEPTUALIZACION DEL DOCUMENTO ELECTRONICO

A) Concepto estructural

No existe un concepto de "documento electrónico" que haya sido adoptado en general por la doctrina y las legislaciones, por lo que para conceptuar el documento electrónico es menester recapitular lo expresado para el documento en general al inicio de este trabajo.

Siguiendo lo sostenido por Carneluti de que el documento es cualquier cosa que represente un hecho,[1] podemos afirmar que estructuralmente el documento puede adoptar diversas formas para su representación material y contiene un elemento intelectual. Lo parte o representación material en la práctica actual está representado por el papel y la parte intelectual conformado como el medio de expresión de su autor.

Frente a la concepción tradicional y con base en las nuevas tecnologías surge en los años ochenta los nuevos soportes y registros en los cuales se plasma la expresión de voluntad mediante datos con sistemas binarios, en soportes magnéticos, ópticos, electrónicos, etc, los cuales necesitan redes de comunicación

[1] Ver supra página 3, CARNELUTTI citado por LARRAUD (Rufino) Op.cit. p. 197

para su transmisión. Esos soportes son los denominados "Documentos Electrónicos".

En un sentido básico, "un documento electrónico es información generada, archivada, enviada, comunicada, procesada, recibida, accesada y desplegada por medios electrónicos."[1]

Surge como el medio en el que las personas manifiestan su voluntad mediante un mensaje de datos en un ambiente de sistemas de comunicación digital o electrónico, produciéndose la denominada "**desmaterialización del documento".**

Esta desmaterilización se da por cuanto el documento electrónico es el "equivalente funcional" al documento escrito concebido en medios análogos (escritura y papel), ya que está contenido en un medio tangible o es almacenado en un medio electrónico a los que se puede acceder, sustraer y desplegar en forma perceptible.[2]

Esta información puede ser de diferentes tipos: datos, textos, voz, imágenes, sonidos, video, software y cualquier otras especie simbólica con significados concretos, siempre que sean realizados en medios electrónicos.

---

[1] AGUILAR SÁNCHEZ, (Edwin). Reglas Generales para las Firmas, Certificados y Contratos Digitales. Op. Cit. p. 2

[2] En este sentido el artículo 2 inciso 10) del Proyecto de Ley sobre Firmas Digitales y Certificados Digitales dispone como documento "información que se encuentra almacenada en un medio tangible o que se guarda en un medio electrónico o de cualquier naturaleza y que se puede recuperar o reproducir en un forma perceptible e inteligible."

La desmaterilización no influye en la introducción del proceso intelectual de la persona que lo crea, pues la intelectualidad constituye la razón de ser de la confección documental.

Se ha distinguido este documento porque "está elaborado en forma digital, a través de un sistema alfanumérico o similar y depositado en un sistema de archivo computacional y cuya información solo puede ser percibida por el ser humano con la intervención de una máquina de traducción a un lenguaje entendible y natural."[1]

Como vemos el documento electrónico tiene estructuralmente los elementos propios del documento en general:

a- Tiene un cuerpo: Aunque es una representación desmaterializada (por ser digital y no estar en un documento atómico o de papel) y diferente a la tradicional.

b- Tiene un contenido: Es la información contenida en el medio electrónico con un significado concreto y querido por su autor.

[1] GAETE GONZALEZ (Eugenio) Firma Electrónica y Firma Digital, 2001. Documento enviado por el Dr. Gaete adjunto a mensaje de correo electrónico dirigido a Kadir Cortés Pérez el 10-02-2002, p. 3.

c- Tiene un autor: La persona que realiza el mensaje de datos y que manifiesta su voluntad por ese medio.

Por lo anterior y siendo el documento electrónico un medio que tiene carácter representativo y declarativo, podemos sostener que desde el punto de vista estructural, es una forma especial de documento que tiene cuerpo (aunque es digital) y representa un hecho, con la diferencia que esta elaborado en un medio electrónico.

B) Concepto funcional.

Funcionalmente el documento es una cosa que sirve para representar otra, que trasladado al campo jurídico serviría para demostrar la cosa representada.

Como analizamos en los fines del documento y principalmente en el documento notarial, su finalidad originaria ha sido evidentemente probatoria., aunque también tiene fines registrales y ejecutivos.

Podremos utilizar un documento electrónico para demostrar lo que se ha representado en ese medio?

En la actualidad y como dijimos antes, el documento se ha desmaterilizado dando lugar a la existencia del documento electrónico, cuyo ser se manifiesta en un lenguaje binario a través de un sistema de conformación electrónica presente en un

hardware que mantiene inalterable el documento en su integridad intelectual. Ese documento puede comprobar la voluntad de la persona que lo realizó.

Para evitar que esa conformación electrónica que contiene una manifestación de voluntad no sea reconocida como un documento, se ha establecido por la Comisión de las Naciones Unidos para el Derecho Mercantil Internacional el principio de "**equivalencia funcional**" para los documentos electrónicos.

Este principio está basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel.

El documento de papel cumple con varias funciones, como son:

a- Proporcionar un documento legible para todos,

b- Asegurar su inalterabilidad en el transcurso del tiempo,

c- Permitir su reproducción y su autenticación mediante la firma ,y

d- Puede ser presentado ante las Autoridades Públicas y Judiciales.

Todas estas funciones pueden ser cumplidas por el documento electrónico, que además puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, observando ciertos requisitos técnicos y jurídicos, otorga

mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos. [1]

La equivalencia funcional no quiere decir que un mensaje de datos sea igual a un documento de papel, ya que son de naturaleza distinta; sino que determina el cumplimiento de criterios que deben ser cumplidos por los mensajes de datos, que le permitan un reconocimiento legal equivalente al de un documento de papel que haya de desempeñar idéntica función.

La desmaterialización del documento ofrece muchas ventajas en la comunicación, pues se da una transferencia de documentos rápida, fluida y comprensible, sin errores, adecuada a la tecnología actual con una enorme reducción de recursos humanos y materiales y con un control y seguimiento antes impensable. Su única desventaja es su falta de regulación legal para dotarlo sin lugar a dudas de plena eficacia jurídica y valor probatorio.[2]

Aunque como veremos en nuestro último capítulo, existen normas que reconocen el uso de documentos electrónicos, la falta de regulación legal expresa del soporte digital del documento electrónico compromete en algunos casos la posibilidad de valorar la prueba en su integridad, autoría e inalterabilidad.

---

[1] Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre el Comercio Electrónico. www.uncitral.org p.15

[2] BARRIUSO RUIZ (Carlos) La Contratación Electrónica. Op. Cit. pp.226 y 227.

Algunos detractores del documento electrónico sostienen la prevalencia del soporte de papel en cuanto a la necesidad de que los documentos electrónicos deben ser trasladados a dicho soporte, dilema que se encuentra superado por la existencia de documentos que únicamente precisan del sistema electrónico informático para su reproducción y del soporte digital para su grabación y no por ello pierden la función de su contenido como expresión simbólica o formal de la voluntad.[1]

Esta nueva forma de documentos que plantea problemas, como los apuntados de la ausencia del soporte en papel, de la firma autógrafa que acredita su autenticidad y la carencia de una legislación específica, plantean la polémica sobre la validez del documento emitido y contenido en un soporte electrónico.

Aún con lo anterior y como una afirmación preliminar con respecto al documento electrónico y al documento en general, para que se le otorgue validez es necesario que tenga valor probatorio; es decir, que por medio de él se logre demostrar algún hecho o circunstancia relevante para el Derecho.

Varios países de América ya han incluido normas que reconocen la admisibilidad de los documentos electrónicos y en Europa son múltiples las Directivas comunitarias que impulsan a las legislaciones nacionales a incluirlas

[1] BARRIUSO RUIZ (Carlos) La Contratación Electrónica Op. Cit. p.234.

dentro de su legislaciones para ser utilizados indistintamente con el soporte de papel.

Los primeros esfuerzos se hacen para dotar al documento electrónico de una codificación que permita que su usuario esté protegido de riesgos, especialmente criminales, por lo cual desde un punto de vista jurídico, se recurrió a su protección penal y civil y desde el punto de vista técnico, se establecieron códigos secretos conocidos solo por el usuario con el fin de impedir la violación documental.[1]

Sección II: VALOR PROBATORIO

Desde un punto de vista jurídico, la razón de ser de todo documento es demostrar lo que representa. Este fin es aplicable también al documento electrónico o digital.

Para que el documento electrónico pueda servir como medio de prueba ante estrados judiciales u oficinas administrativas, debe ser reconocida por ley.

Es plenamente reconocido que "el documento electrónico ha sido admitido por la sociedad, desde hace tiempo, como un medio por el cual comunicarse, guardar información o realizar y confirmar transacciones, entre otros. Sin embargo, toda la confianza depositada en el documento electrónico, fundamental

[1] GAETE GONZALEZ (Eugenio) Firma Electrónica y Firma Digital, Op. Cit., 4

para la realización de comercio "on line", podría tambalearse si dichos documentos electrónicos careciesen de valor probatorio ante los tribunales o ante cualquier otro organismo que resuelva conflictos extrajudicialmente." [1]

En nuestro país existen normas dispersas que reconocen la posibilidad de utilizarlos como prueba, pero su incorporación al proceso queda sujeta al prudente arbitrio y a la valoración que realice el Juez (Art. 368 CPC).

Es por ello que para que se le reconozca plena fuerza probatoria a los documentos electrónicos, es necesario una ley que, en aplicación del principio de equivalencia funciones, los asimile a los documentos en papel.

Los medios de prueba deben estar acordes a la expresión de la realidad social, por lo que es necesario que los medios electrónicos de información utilizados para la creación de documentos estén plenamente reconocidos por ley.

Para que en Costa Rica se dé un desarrollo exitoso del comercio electrónico, es necesario que los documentos electrónicos estén plenamente reconocidos por ley y tengan fuerza probatoria eficaz de lo que representan, siempre que se pueda certificar su autenticidad y fidelidad.

---

[1] CERVELLO GRANDE (José Maria) La prueba y el documento electrónico. Derecho de Internet, Contratación electrónica y firma digital. España, Editorial Aranzadi S.A., 1° Edición, 2000, p. 385.

Esto se fundamenta en la naturaleza jurídica del comercio electrónico, el cual no se basa en relaciones de confianza entre las partes que contratan, por cuanto en ocasiones ni siquiera se conocen físicamente y no hay apreciación subjetiva de la contraparte, convirtiéndose el documento electrónico en la única fuente de seguridad para las partes. Por lo tanto, es importante demostrar su validez probatoria ya que en caso de negársele es muy probable que las relaciones comerciales electrónicas pierdan la fuerza con la que se han venido desarrollando hasta la fecha.[1]

La prueba es en nuestro sistema, uno de los temas de mayor importancia en la norma procesal, en la doctrina, en la jurisprudencia y sobre todo en la práctica, por ser la fuente que sirve para la resolución de los procesos.

Es común escuchar voces contrarias al uso de documentos electrónicos como medio de prueba, por cuanto no hay forma de presentar un original. Esto se soluciona estableciendo la equivalencia funcional de que cuando se reproduzca el documento por diversos procedimientos técnicos de manera que se puede acceder,

[1] Se volvería a la situación que se dio cuando se inicio el comercio electrónico a nivel mundial, donde habían problemas con el anonimato, la falta de firmas, la falta de identificación de las partes y la falta de seriedad en el cumplimiento de los contratos.

sustraer y desplegar en forma perceptible reduciendo los problemas de alteración, el mismo se debe considerar como "original".[1]

La Procuraduría General de la República ha dictaminado que actualmente los documentos electrónicos son fuente de "prueba", independiente de su carácter de prueba preconstituida Sostiene que su incorporación al proceso, con las diligencias a que pueda dar lugar, está determinada por la actuación del Juez que lo incorpora al proceso.[2] Lo anterior quiere decir que si el Juez no la incorpora no se le da el valor probatorio per se, que como documento debería ostentar.

Por el avance que se ha dado en España en este tema, es importante indicar algunos ejemplos de resoluciones judiciales de los Tribunales Españoles, que han determinado la eficacia probatoria del documento electrónico, equiparándolo al documento escrito siempre que se pueda certificar su autenticidad, veracidad y fidelidad .

"La Sentencia de 8 de noviembre de 1.993 de la Audiencia Provincial de Badajoz, "*admite como prueba una factura en SOPORTE INFORMÁTICO aportada por la ejecutante.*

---

[1] Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre el Comercio Electrónico. Op.Cit. p.28

[2] Procuraduría General de la República, Dictamen C-283-98, dirigida al Archivo nacional el 24 de Diciembre de 1998.

La Sentencia de 14 de noviembre de 1.994 de la Audiencia Provincial de Badajoz, *"señala archivos y registros INFORMÁTICOS contables, para expedir las certificaciones.*

La sentencia de 20 de julio de 1.994 de la Audiencia Provincial de Toledo, *" admite el documento electrónico en el sistema nacional de compensación electrónica.*

LA JURISPRUDENCIA DEL T.C. y del T.S., admite como medios de prueba los documentos electrónicos expresados por sistemas informáticos electrónicos o telemáticos, siempre que sean auténticos y se hayan obtenido lícitamente....la SENTENCIA DE 5 DE FEBRERO de 1.988 Sala 2 (RA 857) indicaba, que las innovaciones tecnológicas -vídeo, cinta magnetofónica, ordenadores electrónicos... etc.- pueden y deben incorporarse al acervo jurídico procesal en la medida en que son expresiones de la realidad social que el derecho no puede desconocer."[1]

El objetivo primordial del reconocimiento legal, y por tal valor probatorio, del documento electrónico es evitar la indefensión, que se podría presentar cuando una de las partes alegue el desconocimiento y validez de dicho documento.

En un sistema de derecho como el nuestro en que la defensa es uno de los derechos fundamentales y primordiales de toda persona que acude a los Tribunales en busca de justicia, deben ser protegido por medio de pruebas válidas,

[1] BARRIUSO RUIZ (Carlos) Op.Cit. p. 314

claras y legales. Dentro de dichas pruebas podríamos encontrar al documento electrónico, por lo que el reconocimiento del documento electrónico para ser utilizado como medio de prueba en defensa de derechos en el representados, es imprescindible.

El Tribunal Supremo Español emitió una resolución muy interesente el 03 de Noviembre de 1997 (RJ 1997, 8252) por ser la primer sentencia española que da validez probatoria a la firma electrónica. Esta resolución hace una alocución a la realidad de su país, en ese momento, del documento electrónico al expresar:

> *"Estamos asistiendo, en cierto modo, en algunas facetas de la vida, incluso jurídica, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. El documento, como objeto corporal que refleja una realidad fáctica con trascendencia jurídica, no puede identificarse, ya, en exclusiva, con el papel como soporte, ni con la escritura, como unidad de significación, El ordenador y los ficheros que en él se almacenan constituyen, hoy día, una nueva forma de entender la materialidad de los títulos valores y, en especial, de los documentos mercantiles... En consecuencia, aunque, al igual que en el caso de los documentos comunes, puede haber documentos*

sin firma, el documento electrónico (y, en especial, el documento electrónico con función de giro mercantil) es firmable, en el sentido de que el requisito de la firma autógrafa o equivalente puede ser sustituido, por el lado de la criptografía, por medio de cifras, signos, códigos, barras, claves u otros atributos alfa-numéricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido."[1]

Esta sentencia constituyó un paso decisivo y fundamental para la admisibilidad, en el ordenamiento jurídico español, de procedimientos de autenticación electrónicos de documentos emitidos mediante el empleo de técnicas EIT (Electrónicas, Informáticas y Telemáticas).

Luego de dicha resolución, que inicio la aceptación jurisprudencial de dichos mecanismos como prueba procesal, el problema de la autenticidad en el ordenamiento español se resolvió definitivamente con la aprobación del Real Decreto-Ley 14/1999, e incluso con carácter previo por el Real Decreto 1290/1999.[2]

---

[1] RIBAS ALEJANDRO (Javier) Aspectos Jurídicos del Comercio Electrónico en Internet, España, Editorial Aranzadi, 1° edición, p. 107-109, citando la Sentencia STS 3 de noviembre de 1997 (RJ 1997, 8251, resolviendo sobre los impuestos sobre transmisiones patrimoniales y actos jurídicos documentados

[2] ALCOLEA (José Miguel) La Incorporación de las técnicas electrónicas, informáticas y telemáticas a la actividad de la Administración del Estado Español. Derecho de Internet. Contratación electrónica y firma digital. España. Editorial Aranzadi S.A., 1° edición, 2000, P.573

La referencia de estas sentencias son importantes para nuestro país, ya que aunque a pesar de recoger la realidad española, la misma no es extraña a nuestro medio.

Hemos aplicado a este análisis una tesis analógica de los documentos electrónicos, cuya validez debe interpretarse por medio de reglas de la sana crítica a la luz de los avances de la tecnología, sin tomar en cuenta que algunas normas permiten el uso de documentos realizados por medios electrónicos, lo cual analizaremos en el último capítulo.

Sección III- VALIDEZ DEL DOCUMENTO ELECTRONICO

En el análisis de la validez del documento electrónico debemos encontrar los elementos suficientes por los cuales la información generada, archivada, enviada, procesada y desplegada por medios electrónicos sea considerada como un "documento".

La posición actual dirigida a otorgar validez al documento electrónico, como equivalente funcional del documento escrito, fue incluida por la Procuraduría General de la República en un dictamen que "afirma que no hay inconveniente para considerar el documento electrónico, como documento escrito, ya que:

1. Contiene un mensaje (texto alfanumérico o diseño gráfico).
2. Está escrito en lenguaje convencional (el de los bits).
3. Está sentado sobre soporte material (cinta o disco); y
4. Está destinado a durar en el tiempo." [1]

En el proceso de creación del documento electrónico existe un soporte y existe un conjunto de signos recogidos y adheridos al referido soporte; elementos que pueden magnetizarse o recoger huellas ópticas susceptibles de determinar cual es el contenido de la información.

Lo característico de este documento, es que los signos plasmados en él no son susceptibles de entendimiento por el hombre, sino hasta después de un complejo proceso de descodificación, inverso al de su creación.

Además la validez está relacionada con los criterios de seguridad que permiten al documento electrónico constituirse como documento propiamente dicho, dentro de los cuales se han señalado los siguientes:

1- Ser inalterable,
2- Ser legible mediante un procedimiento apropiado,
3- Ser identificado respecto del lugar, tiempo y espacio de su origen, y

[1] Procuraduría General de la República. Dictamen C-283-98. Op.cit.

4- Ser estable, lo que plantea el problema del soporte físico y los métodos para su mantenimiento en el tiempo[1].

Por último el documento debe ser legal, a fin de incorporarlo dentro de la categoría de los actos jurídicos, y en especial como una nueva forma de contratar sobre las ya existentes: oral y escrita, a las que se sumaría la electrónica.

Debe quedar establecido que ante la existencia de un documento informático y afín de dotarlo del debido valor jurídico y especialmente probatorio, se le debe aplicar un sistema de encripción para otorgarle seguridad.

La compatibilidad jurídica entre el documento escrito tradicional y uno electrónico debe ser plena, ya que el objeto jurídico para determinar su validez será independiente a la forma en que se plasme la formación de la voluntad y el consentimiento. En la representación formal influyen los medios que la tecnología ofrece en cada momento cuyo problema no será la determinación de la validez o no de su forma o soporte, sino el empleo de medios lícitos para determinar la autoría y autenticidad en sede judicial en caso de conflictos.[2]

Solamente mediante la promulgación de una ley se puede establecer el **principio de equivalencia funcional** del documento electrónico y el escrito[3]. Esta

---

[1] Ibid.
[2] BARRIUZO RUIZ (Carlos) Op. Cit. p. 321
[3] Esta ley debe seguir la recomendación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

equivalencia se logra determinando los criterios que debe cumplir un mensaje de datos (documento electrónico), para que se le atribuya un reconocimiento legal equivalente al de un documento de papel que haya de desempeñar una función idéntica.

Una vez establecido dicho principio, debemos asimilar la validez de los documentos electrónicos con los documentos escritos, por contar con características propias que los hace desempeñar una idéntica función de autenticidad y/o veracidad, lo cual se logrará con el reconocimiento de la firma digital.

CAPÍTULO SEGUNDO

LA FIRMA DIGITAL

SECCIÓN I: MÉTODOS CRIPTOGRÁFICOS

Si la seguridad en internet es lo que más preocupa a sus usuarios, en cuanto a la privacidad de la información, el tema es de prioridad en cuanto a la contratación electrónica, el notario cibernético y el protocolo electrónico.

Con los avances en tecnología, la información que viaja por las redes, nodos, links o routers, puede ser susceptible de ser interceptada o manipulada mediante el acceso ilegal de los hackers o crakers que tienen el conocimiento para romper las protecciones utilizadas.

En nuestro campo y una vez que entremos a realizar la función notarial digital, debemos conocer estos riesgos y las técnicas que se deben utilizar para dar mayor seguridad y confidencialidad a la actuación notarial electrónica y en sí a la contratación electrónica.

Como explicamos en el capítulo correspondiente al TCP/IP, para evitar un colapso por saturación de un canal, la información viaja en datagramas y en un lenguaje binario. Es así como todos los datos que genera la contratación electrónica, al igual que cualquier otra, al final no es más que información binaria.

Como toda información binaria (bits: unos y ceros), la contratación electrónica debe ser protegida atendiendo a niveles de clasificación definidos por un entorno fiable de seguridad, privacidad, identificación, autoría e identificación.

La seguridad en internet en general[1] está referida a la protección física y principalmente a la integridad de los datos y la disponibilidad de los mismos.

Particularmente para los notarios, el tema de la seguridad jurídica en el tráfico de la información en las redes para dar certeza a la contratación es primordial.

Como la contratación electrónica no es más que información binaria, debemos, en principio, valernos de los medios técnicos existentes. Uno de los sistemas que existen que ha resultado más eficaz es la firma digital.

"La firma digital es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quien es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad)"[2]

La seguridad del sistema utilizado en la firma digital descansa en el cifrado del documento con una clave, utilizando un sistema criptográfico.

---

[1] Supra Sección III, Capítulo I, Título II.
[2] RAMOS SUAREZ (Fernando) Como aplicar la nueva normativa sobre Firma Electrónica.www.legalia.com, documento sin numeración de página

La criptografía es una de la ramas de la criptología que en general estudia la seguridad de las comunicaciones y de las técnicas para cifrar y descifrar comunicaciones secretas.

Generalmente se ha definido como "la ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones."[1]

Cuando desarrollamos el tema de la Criptografía en la Informática en General, expusimos que se trata de los métodos y técnicas de encripción y decripción de comunicaciones al servicio de la seguridad.

Como tal la criptografía es el conjunto de técnicas matemáticas y computacionales para la protección de datos, comunicaciones y transacciones, que ofrece tres tipos de servicios de seguridad, a saber:

a- Autenticación: Verifica la identidad del transmisor del mensaje (identificación) y la integridad del mensaje.

b- Certidumbre: Provee evidencia cierta de una transacción (non repudiation).

[1] DE LA FUENTE (Juan Ángel) La Contratación Electrónica, la Criptografía y la Firma Digital, en Revista Internacional del Notariado, ONPI, Buenos Aires, N° 96, Segundo Semestre, 1998, p. 173.

c- Privacidad: Protege la información de ser conocida por personas no autorizados o no legítimas.[1]

Estas técnicas complementan la arquitectura de seguridad de las comunicaciones de los usuarios de la red Internet, del modelo OSI de la Intenational Standard Organization.

La encripción se basa en dos elementos cruciales: un Algoritmo criptográfico (que sería una función matemática) y una clave o llave. Dependiendo del largo de la clave, así será la seguridad que ofrezca la encripción que se realice.

Para encriptar se toma el texto del mensaje y se le aplica una función matemática con la llave, produciéndose un texto cifrado. Este proceso hace que el texto cifrado sea incomprensible para un tercero que desconozca la llave decodificadora, pues únicamente con dicha llave el texto cifrado puede verse como era originalmente.

En la encripción se dan dos tipos de sistemas o tecnologías:

a- La Encripción Simétrica o de Clave Secreta; y

b- La Encripción Asimétrica o de Clave Pública.

Veamos que nos ofrecen estos dos tipos de tecnologías.

---

[1] AGUILAR SÁNCHEZ (Edwin) Economía Digital, Op.cit, documento sin numeración de página.

que tendríamos un número de llaves igual a todas las personas con las que deseamos transmitirnos información .

El sistema más usado de clave secreta de esta modalidad es el DES (Data Encryption Standard), desarrollado por IBM, que utilizada una llave de 56 bits, seguido por el IDEA (International Encryption Algorithm), cuya llave es de 128 bits.[1]

Este sistema es muy poco usado para la firma digital, sino únicamente para comunicaciones dentro de una misma empresa, donde puede ser útil.

No nos extendemos en el desarrollo del sistema simétrico, ya que debido al largo de la llave utilizada, no es un sistema muy seguro para la contratación y la intervención notarial electrónica .

B) Encripción asimétrica

Este es un Sistema creado en 1976 en la Universidad de Stanford y mediante la cual cada persona tiene un par de "llaves": una será pública y la otra será privada. Con este sistema se evita el problema de seguridad del sistema simétrico de tener que enviar la llave por el sistema, por lo que no hay peligro de que un tercero la intercepte.

---

[1] BARRIUSO RUIZ (Carlos), Op.cit. p. 245.

"La llave pública de cada persona es conocida por todos quienes quieran conocerla; en cambio, la llave privada es mantenida en riguroso secreto por su propietario. "[1]

Hay un par de llaves que están asociadas, por lo que cuando una encripta la otra decripta. La llave pública es ampliamente divulgada, sin riesgos y la privada es secreta, por lo que solo la conoce el usuario.

Se provee confiabilidad del mensaje cuando se encripta con la llave pública y se da autenticidad del autor encriptando con llave privada. [2]

Con este sistema cualquier persona puede enviar un mensaje confidencial con sólo utilizar su clave pública, pues el mensaje solo puede decriptarse con la clave privada que posee el receptor. El algoritmo matemático permite encriptar el mensaje con una llave que produce un texto cifrado, difícil de decriptar si no se tiene la llave asociada.

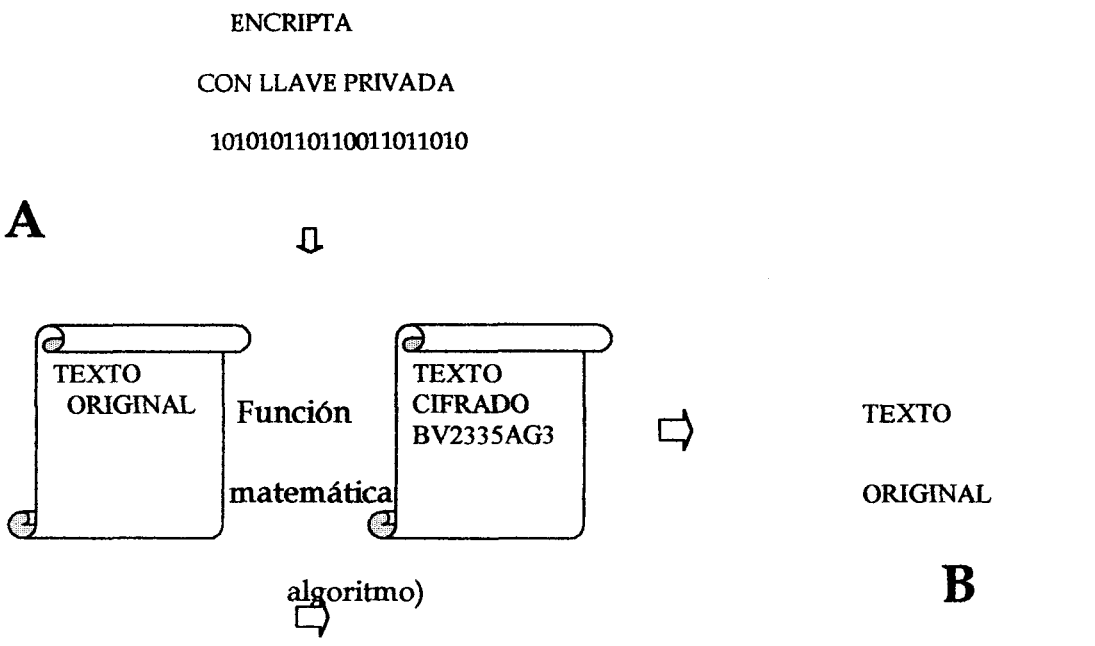
El hacer ininteligible el mensaje, preserva la confidencialidad del mismo, permitiendo determinar la autoría del texto, su integridad y autenticar su contenido.

---

[1] DE LA FUENTE (Juan Angel). Op.cit. p174.
[2] AGUILAR SANCHEZ (Edwin) Economía Digital, Op.cit., documento sin numeración de página

Al contrario del sistema simétrico, el sistema asimétrico no es reversible lo cual impide que se pueda conocer la llave privada a partir de la llave pública y que lo cifrado con la llave pública solo puede descifrarse con la llave privada asociada.[1]

Veamos un ejemplo grafico:



[1] AGUILAR SANCEHZ (Edwin) Economía Digital, Op.cit., documento sin numeración de página

A quiere enviar un mensaje cifrado a B. Cifra el texto con su clave privada y luego se envía con la clave pública de B, así solo podrá descifrarse con la privada de B y con la pública de A.

Como sabemos a quien pertenece la clave pública? Aquí entra en juego una figura que es muy importante en nuestro tema que es la Autoridad Certificadora, pues será dicha autoridad la que indica a quien pertenece la clave pública y es con esa clave que se sabe ciertamente quien es el emisor del mensaje.

El Criptosistema de llave pública más usado es RSA (por las siglas de sus autores: Rivest, Shamir y Adlerman), desarrollado en el Instituto Tecnológico de Massachussets en 1977.[1] Además el sistema PGP (Pretty Good Privacy) está basado en la compresión de datos zip y en RSA, que se distribuye gratuitamente en internet por "ftp" (freeware) o en muchas BBS (Bulletin Board Systems) para paquetes e'mail con algoritmo RSA o IDEA con intercambio RSA o KEA.[2]

Para la contratación electrónica y para el futuro de la función notarial electrónica, este sistema de cifrado asimétrico es fundamental, pues como base de la firma digital otorga integridad y autenticación.

---

[1] Para un mayor desarrollo de es sistema puede consultarse el sitio: **www. rsa.com**
[2] BARRIUSO RUIZ (Carlos), Op.cit. p. 246.

SECCIÓN II: FUNDAMENTOS DE LA FIRMA DIGITAL

"Las firmas electrónicas o digitales consisten básicamente en la aplicación de algoritmos de encriptación a los datos, que de esta forma, solo serán reconocibles por el destinatario, el cual además podrá comprobar la identidad del remitente, la integridad del documento, la autoría y autentificación, preservando al mismo tiempo la confidencialidad. "[1]

Como hemos dicho la seguridad del algoritmo tiene relación directa con el tamaño de su llave, además al tiempo de cifrado y a la no violación del secreto.

Las llaves públicas utilizadas que permiten una encriptación segura son superiores a los 128 bits, que generalmente son de 512 bits, por ser las únicas llaves exportables. Además existen llaves de 768 bits (personal), de 1024 bits (comercial) de 2040 bits (militar), los cuales en este momento no son exportables.[2]

Se habla de llaves exportables y no exportables, por cuanto se tiene por aceptado que por el nivel de seguridad que otorgan los sistemas criptográficos son considerados instrumentos de alto valor estratégico. Por lo menos en Estados

---

[1] BARRIUSO RUIZ (Carlos), Op. Cit. p. 249.

[2] AGUILAR SÁNCHEZ (Edwin) Economía Digital, Op.cit. documento sin numeración de página. Para tener un idea gráfica que como sería una llave segura de 512 bits, el Msc Aguilar Sánchez nos da un ejemplo de llave segura de 512 bits cifrada de manera exadecimal, que sería: 3048 0241 00D6 EFD5 BD41 D116 1DBD CD3F CF91 6801 B238 879F E226 0AD2 6CAD 6CO6 7225 5E96 90AE 43C5 2438 513 0B95 C8C8 D960 9FC3 F926 7005 6DCE A0E8A336 21FC 5BD5 4D3D9702 0301 0001.

Unidos y Francia se llega al punto de ser tratados como "material bélico" sujeto a las prohibiciones y limitaciones de exportación que son típicas del armamento sofisticado.[1]

Para el autor Carlos Barriuso, la firma digital es más segura que la firma ológrafa, pues es inimitable y tiene más elementos que esta. Este autor sostiene que además de aportar la autoría y la conformidad de quien firma, la digital aporta integridad, identidad, autenticidad, datación y autenticación[2]

Los criptosistemas de llave pública son los aptos para la firma digital, por ser técnicamente más resistentes para ser descifrados. Esta resistencia y seguridad se basa en el absoluto secreto que se tenga al generar y guardar la llave privada y en la certificación de la llave pública por la autoridad certificadora.[3]

La integridad e individualización del documento y su función de sellamiento que puede incluir la fecha, el lugar, la hora, el destino, etc., se pueden incluir con la firma electrónica.

Como vemos la infraestructura de la firma digital se basa en utilizar llave pública y llave privada y no se trata técnicamente de una firma, sino de un

---

[1] LOPEZ CEBADA (Juan Jesús) Breves Consideraciones sobre las Posibilidades Subyacentes en la Firma Electrónica Avanzada, 1999, España. En Revista Electrónica de Derecho Informático, www.publicaciones. derecho.org/redi Esto se ha comprobado con la polémica surgida en torna al sistema de encriptación Preetty Godd Privacy (PGP).
[2] BARRIUSO RUIZ (Carlos) Op.cit., p.250.
[3] Ibid.

verdadero sello informático que asegura la integridad del documento y la identidad del usuario.

Después de explicar el sistema de cifrado asimétrico y su función para la firma digital, salta la pregunta lógica: Que es una firma digital?

Existen tres tipos de firma digital o firma electrónica: Si la firma se obtiene con tecnología de criptografía, entonces también se llama firma numérica, porque lo que se obtiene es un número único e irrepetible.

Si la firma se obtiene mediante dispositivos de reconocimiento biométrico (huella dactilar, iris) se denomina firma biométrica.

Por último existe la firma autógrafa digital, que es una firma manuscrita sobre un tablero que la digitaliza y le hace una función de hash.[1]

Para nuestro objeto de estudio nos interesa el primer tipo de firma digital o sea la firma numérica.

La firma digital se produce mediante un procedimiento de encripción, que traduce el documento en una serie numérica única llamada DIGESTO, por medio de un algoritmo o función de **hash**[2]. El digesto se encripta con clave privada, dando como resultado la **firma digital.**

---

[1] AGUILAR SÁNCHEZ (Edwin) Reglas Generales para las Firmas, Certificados y contratos Digitales, Seminario de Notariado Digital, Registro Público de la Propiedad, 2001, documento sin numeración.

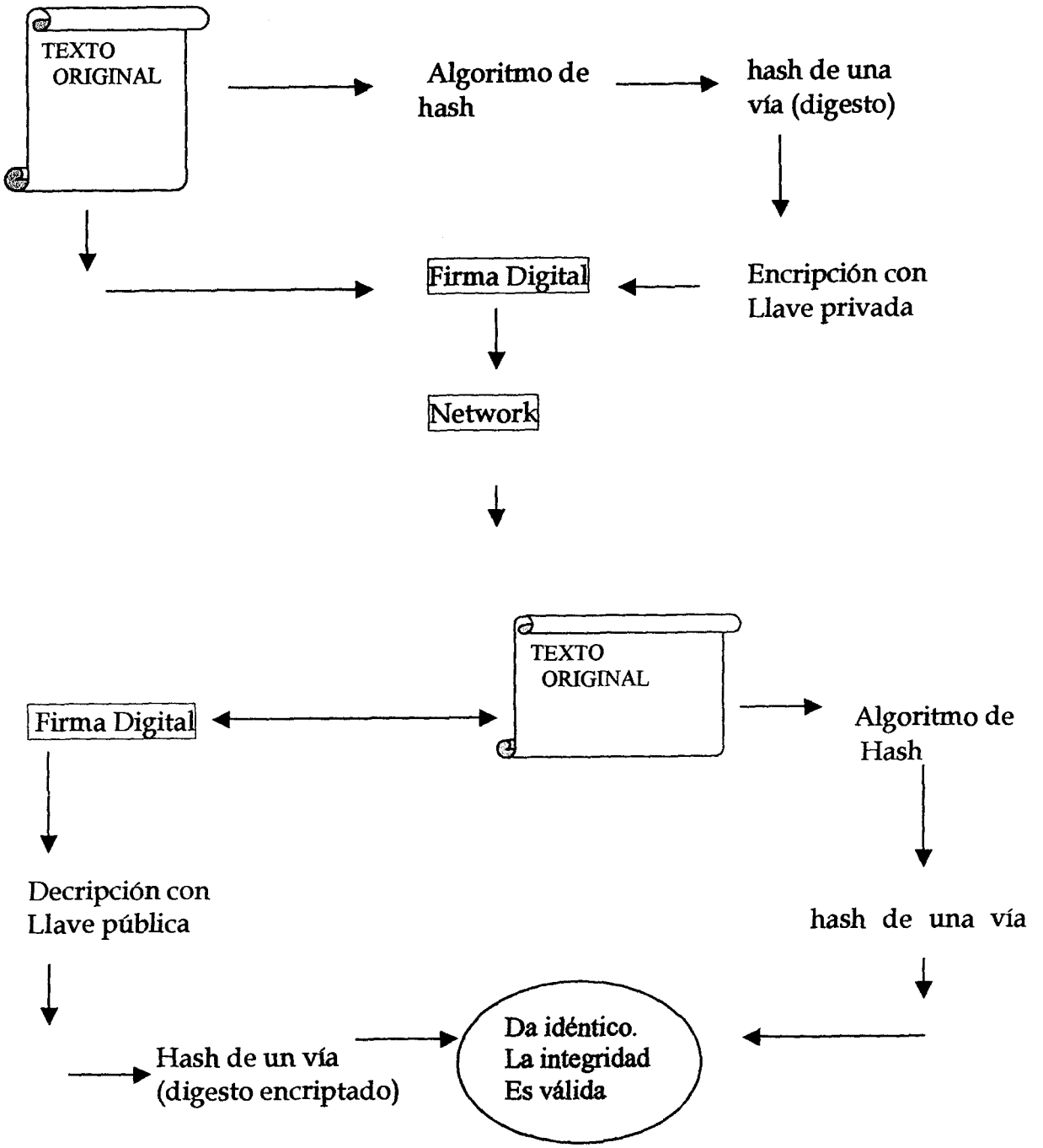
[2] Para comprender la firma digital es importante entender que cuando se habla de "**Hash**", se trata de una técnica matemática que analiza un documento o texto y le asigna un número matemático único.

Como se aplica ese algoritmo al texto? Es el software del firmante el que aplica el algoritmo sobre el texto que se firma, obteniendo un extracto de longitud fija y específico para ese mensaje.

El Msc Edwin Aguilar Sánchez también sostiene lo manifestado por el autor Carlos Barriuso en cuanto a que la firma digital es más segura que la ológrafa. La firma ológrafa es siempre la misma y con la práctica se puede imitar, pero la firma digital no, pues cambia con cada texto o documento cifrado ya que cada vez dará un número diferente dependiendo de los valores asignados al documento. Lo único que se mantiene es la clave privada.[1]

Se podría pensar que si obtengo el digesto podría llegar al texto, lo cual no es posible porque se utiliza hash de una vía que no permite esa función. Como se ha expuesto, se utiliza un sistema no reversible que impide que con el conocimiento de la llave pública se pueda conocer la llave privada.

[1] AGUILAR SÁNCHEZ (Edwin) Economía Digital, Op.cit, documento sin numeración de página.


TEXTO ORIGINAL
Algoritmo de hash
hash de una vía (digesto)
Firma Digital
Encripción con Llave privada
Network
TEXTO ORIGINAL
Firma Digital
Algoritmo de Hash
Decripción con Llave pública
hash de una vía
Da idéntico. La integridad Es válida
Hash de un vía (digesto encriptado)

Como podemos observar en este ejemplo, el software del que envía aplica al documento original un algoritmo de hash y obtiene un digesto. El digesto será diferente conforme el tamaño del texto y el hash es de una sola vía, el cual se encripta con nuestra llave privada con lo que obtenemos una firma digital, la cual se envía con el documento a través de la red con la llave pública del receptor. Esta llave se conoce a través de una Autoridad de Certificación.

El que recibe el documento toma la firma digital y decripta con su llave privada y obtiene el digesto encriptado; a su vez le aplica el algoritmo de hash al documento y obtiene el digesto de ese documento. Si ambos digestos son idénticos, el documento no fue alterado, por lo que su integridad está garantizada y su autoría no es repudiable, pues mi identidad se logra corroborando mi clave pública con la autoridad de Certificación.

Como sabemos que el digesto logrado con la función de hash no puede ser alterado?

La función da un número matemático que resulta de sumar los valores ascii por posición; las consonantes, las vocales, los signos de puntuación y los espacios en blanco tienen un valor.

La función de hash es tan exacta que la suma del texto da un número único, en el que no se puede quitar ni variar un espacio en el texto, pues daría la suma de

otro número y el texto sería repudiable.[1] Un mínimo cambio en el mensaje produce un extracto completamente diferente, por lo que no correspondería con el que originalmente se firmó.

La utilidad y la fortaleza de una función de hash o sellamiento, como pilar de la firma digital, está en que es imposible generar dos resúmenes numéricos iguales, partiendo de documentos similares y mucho menos de dos documentos distintos.

Además el mensaje cifrado mediante hash lleva una función de sellamiento, que indica la fecha y la hora en que se envió el mensaje, el cual no puede ser alterado.

En otro frente y para evitar que alguna de las partes argumente que no ha recibido el documento, se establecen las "pruebas de no repudio" y los "acuses de recibo electrónico"[2] con la intervención de terceras personas confiables que hacen prueba del envío o recepción del documento en su hora y día concreto. Inclusive esta tercera persona puede encriptar el mensaje recibido con su propia clave

---

[1] AGUILAR SÁNCHEZ (Edwin) Economía Digital, Op.cit. documento sin numeración de páginas

[2] La Ley Modelo de la CNUDMI sobre Comercio Electrónico, propone en su artículo 14, varias formas de acuse de recibo por la utilidad que ello conlleva a la actividad comercial, el cual va desde un simple mensaje de acuse de recibo que no significa la aceptación de una oferta que se ha recibido, hasta el acuse de recibo con la manifestación de un acuerdo con el contenido del mensaje. Será la legislación nacional siguiendo el derecho de los contratos la que determinará los alcances del acuse de recibo y la intervención de los notarios públicos como terceras personas confiables, cuando el acto lo requiera.

privada y enviándolo a las partes, haciendo que opere como prueba iuris et de iure.

Luego de utilizar los medios de seguridad se hace necesario garantizar al emisor y al receptor, que son quienes dicen que son, lo cual se logra con estas terceras personas confiables denominadas Autoridades o Entidades de Certificación Electrónicas, quienes serán los que certifiquen y autentiquen a las partes. Estas entidades serán encargadas de otorgar autenticación a firmas y certificados digitales, precisando el plazo de su validez.

Entratándose de contratación, la figura del Notario Público es la que debe intervenir como parte de esa tercera parte confiable. Será la ley que autorice a los proveedores de servicios de certificación digital o su respectivo reglamento, quien requiera la intervención de los Notarios en dichas entidades.

La intervención notarial en la identificación y autenticación de las personas cuando solicitan sus certificados digitales, dará la seguridad de que quien está utilizando la clave es quien la solicito y se identificó ante el Notario.

La Autoridad de Certificación es una empresa que autenticas a las personas en el sistema, pero dicha autenticación viene con el respaldo otorgado por el Notario que identificó plenamente a dicha persona ante la Autoridad; en caso de

personas jurídicas, es el Notario el encargado de corroborar la autenticidad y vigencia del poder que se ostenta.

En caso de contratación y de ser necesario elevar el documento a forma pública, será necesaria también la intervención del Notario que, con su firma digital, lo dotará de medio de prueba irrefutable, solucionando el problema del envío, el recibo del documento, su aceptación o rechazo.

Cuando analicemos la figura del Notario Cibernético, se desarrollará la intervención notarial en el sistema, ya sea, primero como parte de la Autoridad de Certificación, segundo como encargado de solicitar los certificados digitales ante las Autoridades de Registro[1], o tercero, autenticando digitalmente con su firma los documentos electrónicos que lo requieran.[2]

La intervención del Notario en una contratación electrónica es necesaria para garantizar la asociación entre un par de claves y una persona determinada, así como para la distribución efectiva de las claves que las vincule a una persona con la clave pública, que identifique al titular de la clave privada.[3]

Como dijimos será la ley la que determine a quien le corresponde confirmar la identidad de los contratantes en el mundo electrónico. Puede ser algún órgano

---

[1] El Notario Público en México, que cumpla con los requisitos establecidos por ley, puede pertenecer a la Red de Certificación Digital y como tal emitir certificados digitales

[2] Como lo prevé el Proyecto de Ley de Firma Digital y Certificados Digitales de Costa Rica, en su artículo 6.

[3] CORNEJO LOPEZ (Valentino) Una Realidad Mexicana, la Firma Electrónica y la Participación del Notario Mexicano. Op. Cit. documento sin numeración de pagina.

estatal, pero la función sería muy natural para la labor de los Notarios o Cibernotarios.

SECCIÓN II: PRINCIPIOS DE LA FIRMA DIGITAL

Cuando se trata el tema de la Firma Digital se plantean dos problemas: uno es de seguridad tecnológica y otro de seguridad jurídica.

En los sistemas anglosajones la solución al problema de la seguridad jurídica se hace recaer sobre la seguridad tecnológica, por que se pretende que existiendo identificación e invulnerabilidad de la firma, el problema está solucionado.

En los sistemas de notariado latino, esta solución no basta, pues la seguridad jurídica solamente se da con la "fe pública".[1]

La firma digital de un Notario Público será el sustento de la legalidad de los procesos de certificación digital, trasladando al mundo virtual el valor de la fe pública que ejerce en el mundo real.

Insistimos en esta posición porque "una tendencia en materia de certificación electrónica ha sido la creación de los Cibernotarios, aunque en

[1] RECORDER DE CASSO (Emilio) Algunas Observaciones en torno a contratos, electrónica y fe pública. Derecho de Internet. Contratación electrónica y firma digital. . España, Editorial Aranzadi S.A. 1ª. Edición, 2000, p. 118

algunos países, donde existen figuras más amplias como es el caso de los "Fedatarios", se han otorgado facultades certificadoras a todas aquellas personas investidas de fe pública."[1]

Este efecto se da a partir del reconocimiento del "principio de equivalencia funcional" por medio del cual el documento firmado digitalmente tiene la misma validez y eficacia que un documento atómico o en soporte de papel debidamente firmado.[2]

El fin de la firma digital será el mismo de la firma ológrafa: dar asentimiento y compromiso a lo firmado, proveyendo seguridad y confianza a los mensajes o negocios realizados electrónicamente.

Cuando se encripta con llave privada es funcionalmente equivalente a firmar con puño y letra sobre papel y cualquiera que decripta el mensaje con mi llave pública, estará seguro que el mensaje fue enviado por mí.

El comercio electrónico y todo tipo de transacción o acto realizado electrónicamente a través de Internet, se enfrenta a la obtención del mayor grado

---

[1] JIJEMA LEIVA (Renato) Comercio Electrónico y Derecho. La Problemática Jurídica del Comercio Electrónico. Universidad Católica de Valparaíso, 1999. documento sin numeración. www.publicaciones.derecho.org/redi

[2] Siguiendo las recomendaciones de la Ley Modelo de la CNUDMI, este principio esta reconocido en el Proyecto de Ley de Firma Digital y Certificados Digitales de nuestro país que establece en su artículo 1, que la Ley "tiene por objetivo regular el uso y el reconocimiento jurídica de la Firma Digital, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad..."

de seguridad jurídica, el cual puede ser proporcionado con la firma digital en razón principalmente de la confianza en la aplicación de los sistemas criptográficos a los mensajes de datos.

La firma digital establece una serie de principios establecidos por la doctrina, respecto a los fundamentos jurídicos que deben regir una transacción, que serán: **La Confiabilidad, la Integridad, la autenticidad y el no repudio.**

Estos principios establecen presunciones legales que son fundamentales para otorgar seguridad jurídica al tráfico de actos o contratos realizados en el medio electrónico.

Entendamos los principios en que se basa la firma digital:

i- **Confiabilidad**: El objeto principal es que el mensaje solo pueda ser leído por su destinatario o por aquellas personas autorizadas con derecho de acceso a la información. Los sistemas y procedimientos de seguridad de combinación de doble llave garantizan la confiabilidad de los datos firmados digitalmente, de manera que el emisor estará seguro de que solamente la persona a la que va dirigido el mensaje lo pueda leer.[1]

En Europa la confiabilidad o confidencialidad se ha tratado de garantizar desde 1997, con la promulgación de la Directiva 97/66/CE del 15 de Diciembre de

[1] PEREZ PEREIRA (Maria) Hacia la seguridad en el Comercio Electrónico. Revista de Derecho Informático, 1999, www.publicaciones.derecho.org/redi. Documento sin numeración de página

1997, mediante la cual se indica a los Estados que deben prohibir cualquier forma de interceptar o vigilar estas comunicaciones por parte de cualquier personas que no sea su remitente o su destinatario, salvo que este legalmente autorizado.[1]

ii- **Integridad**. Se garantiza que el contenido no ha sido cambiado durante su transito por la red o durante su almacenamiento, de manera que siempre se mantiene en original. Esto no quiere decir que no se pueda alterar, sino que se detecta si ha sido alterado.[2]

El mensaje lleva implícito una presunción de inalterabilidad desde que fue añadida la firma digital, salvo que una de las partes demuestre que hubo una insuficiencia en el procedimiento de seguridad empleado

La integridad es una cualidad imprescindible para darle validez jurídica a la información. La firma digital detecta la integridad de la información que fuera firmada, en forma independiente al medio de su almacenamiento.[3]

---

[1] Directiva 97/66/Ce del 15 de diciembre de 1997, del Parlamento Europeo y del Consejo, relativa al Tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
[2] RIBAS (Xavier) Propuestas de Directiva sobre Firmas Electrónicas. Revista Electrónica de Derecho Informático, 1999, www.publicaciones.derecho.org/redi. Documento sin numeración de página.
[3] ARCE (Alfonso José) DIAZ LANNES (Federico Santiago) La Firma Digital. Aspectos Jurídicos. Su aplicación a las Comunicaciones Previstas por la Ley #22.172, 1979, Revistas Electrónica de Derecho Informático. **www.publicaciones.derecho.org/redi**, página 2

iii- **Autenticidad:** Certeza jurídica sobre la autenticidad del mensaje.

Aquí se da una función de identificación y de autentificación no repudiable de las partes, ya que se garantiza que los sujetos de la transacción o el que transmite el acto electrónicamente, sean quienes se espera que sean. Se presume que la firma digital pertenece a la persona que realizó la firma.

"Esta garantía esta asociada a las normas de custodia de las claves y certificados de cada parte, penalizando un uso o tenencia negligente de los elementos de seguridad que participan en la autenticación de los intervinientes. La carga de la prueba corresponderá a la parte que niegue su intervención en el negocio".[1]

Se puede verificar la identidad del usuario emisor mediante la confirmación de la misma por una tercera parte confiable (Autoridad de Certificación).

Dentro de la autenticidad se encuentra el estampado cronológico (time stamping), aportando la prueba irrefutable de la fecha y hora de la transacción, contribuyendo a evitar una posible repudiación de sus consecuencias legales o de cualquier otra índole.

[1] RIBAS (Javier) Propuesta de Directiva sobre Firmas Electrónicas. Op. Cit.

iv- **No repudio**: Este principio indica que la persona que añadió su firma al mensaje de datos, tiene pleno conocimiento del contenido de la transacción, por lo que el remitente no pueda negar el mensaje de datos que ha enviado.

Con este principio se da certidumbre a la transacción y provee evidencia cierta de lo ocurrido, haciendo que la misma sea no repudiable/no refutable, por lo que garantiza que la transacción ha sido originada por una parte, con el pleno conocimiento y recepción de la otra.

Las partes no podrán rechazar las obligaciones contractuales derivadas del negocio llevado a cabo, salvo en el caso de que demuestren que concurre algún vicio del consentimiento o cualquier otra prueba que desvirtúe la presunción.[1]

La figura jurídica del no repudio surgida en el Common Law, la encontramos cuando un determinado mensaje electrónico adquiere fuerza vinculante o efectos jurídicos, ante el posible rechazo o reclamación de su no existencia.[2]

Este principio no es concebible sin que se dé el principio de la autenticación y el de la integridad, pero es mucho más que autenticidad e integridad.

---

[1] La Directiva 97/7/CE del Parlamento Europeo y del Consejo del 20 de Mayo de 1997, relativa a la Protección de los Consumidores en materia de contratos a Distancia, en su artículo 6 establece un "repudio jurídico" o derecho de desistimiento en un plazo de siete días

[2] RAMOS SUAREZ (Fernando) Eficacia Jurídica de una Transacción electrónica. La figura del No Repudio. www.publicaciones.derecho.org./redi. Documento sin numeración de página.

Con el No Repudio podremos comprobar a una tercera parte que una comunicación específica ha sido realizada, admitida y enviada a una determinada persona. Se comprueba quién envió el mensaje (no repudio de origen) y quién recibió el mensaje (no repudio en el envío)[1].

Como hemos observado, en aras de la seguridad del tráfico mercantil, se introducen a los principios de la firma digital presunciones "iuris tantun", por lo que admiten prueba en contrario. Esto es lógico por cuanto el consentimiento puede estar viciado y los datos pueden haber sido objeto de manipulación no autorizada.[2]

Con base en los principios señalados, diremos que una firma digital se considera fiable si cumple con los siguientes requisitos:

1- Los datos de su creación corresponden exclusivamente al firmante.

2- Los datos de su creación están bajo el control exclusivo del firmante.

3- Es posible detectar si hay alteración posterior al acto de la firma.

4- Cuando garantice la integridad del mensaje firmado y la detección de alteraciones posteriores.

---

[1] RAMOS SUAREZ (Fernando) Eficacia Jurídica de una Transacción electrónica. La figura del No Repudio, Op.cit..

[2] RIBAS (Xavier) Propuesta de Directiva sobre Firmas Electrónicas. Op. Cit.. Las legislaciones europeas que han seguido esta Directiva, como por ejemplo la Italiana, establecen que el documento electrónico firmado digitalmente es oponible iuris tantum a la contraparte y a los terceros.

5- Es compatible con normas o estándares internacionales reconocidos.[1]

Se debe dar validez a la firma digital y lograr su equivalencia a la firma holográfica, otorgándole los mismos efectos legales, por lo que una persona podría usar una firma digital para cualquier propósito requerido o permitido por ley.[2]

Las excepciones que algunas legislaciones señalan para el uso de la firma digital se refieren al Derecho Sucesorio, de Familia, Notarial de Propiedad Inmobiliaria, de Seguros, de constitución, Disolución y Liquidación de personas jurídicas, etc. Asimismo se establecen excepciones para actos jurídicos o contratos para los cuales otras leyes exigen expresamente que se realicen en escritura pública o requieran de la concurrencia personal en ese acto.[3]

En este punto, en Perú la Lic. Carmen Velarde Koechlin ha sostenido que "el Fedatario Juramentado no puede consignar escrituras públicas, ni actos de transferencias de bienes muebles registrables, etc., dejando su labor al proceso de

---

[1] AGUILAR SÁNCHEZ (Edwin) Reglas Generales para las Firmas, Certificados y Contratos Digitales. Seminario: Notariado Digital, San José, Costa Rica, Mayo, 2001, p.8. e IRIARTE AHON (Erick) Firma Digital y Certificado Digital. El Proyecto Peruano. Revista Electrónica de Derecho Informático, 1999 www.publicaciones.derecho.org7redi. Ambos destacando la Propuesta de Directiva del Parlamento Europeo y del Consejo de la Comunidad Europea sobre firma electrónica del 13 de Mayo de 1998.

[2] El artículo 1 del Proyecto de Ley de Firma Digital y Certificados Digitales, establece la equivalencia funcional de la firma digital, siguiendo la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

[3] AGUILAR SÁNCHEZ (Edwin) Reglas Generales para las Firmas, Certificados y Contratos Digitales, Op. Cit. p. 9. El artículo 9 de la Directiva 2000/31/Ce del 8 de Junio del 2000, del Parlamento Europeo y del Consejo en cuanto a los contratos por vía electrónica , incluye una lista similar de contratos que no pueden se realizados electrónicamente.

micrograbación, o sea al traslado de documentos en papel al formato digital, cuya integridad se garantiza con actos de apertura y cierre.[1]

En Chile, la ley homologa el documento electrónico con los de soporte material de papel, reconociendo el derecho de celebrar actos y contratos electrónicos "salvo excepciones legales expresas que requieran documento con formato de papel o la comparecencia personal de alguna de las partes, situación en la cual la exigencia sólo se cumplirá con estos últimos."[2]

En nuestro país el reconocimiento de la firma digital y de los certificados digitales, está en el proyecto de ley presentado por el Poder Ejecutivo por iniciativa del Ministerio de Ciencia y Tecnología.[3] Este proyecto no hace excepciones al uso de la firma digital, entendiéndose por tal que podrá ser utilizada en cualquier acto. Habrá que esperar si por vía reglamentaria se impondrán algunas de las excepciones apuntadas, pues el Ministerio de Ciencia y Tecnología ha manifestado que se trata de un proyecto sencillo, cuyos tecnicismos se reservarán para el reglamento que deberá redactarse posteriormente, pues "lo fundamental de esa ley

---

[1] VELARDE KOECHLIN (Carmen) El Fedatario Particular Juramentado en Informática: Institución Peruana al Servicio de una solución Global, 2000, www.publicaciones.derecho.org/redi, página 18

[2] SANDOVAL LOPEZ (Ricardo) Comentarios Sobre el Proyecto Relativo al Documento y Firmas Electrónicas, 1999, , www.publicaciones.derecho.org/redi, documento sin numeración de página.

[3] Proyecto de Ley de Firmas Digitales y Certificados Digitales, del 22 de Febrero del 2001, Expediente #14276 de la Asamblea Legislativa.

es que documentos digitales puedan tener validez legal y eso ayudará en el desarrollo del comercio electrónico."[1]

Aunque al aprobarse la Ley de Firmas y Certificados Digitales, se establezcan limitaciones o excepciones para el uso de la firma digital, queda un ámbito muy amplio de actos jurídicos y contratos, sobre todo comerciales, en los que será necesaria la intervención Notarial.

Como hemos expuesto, podrá ser parte de las Autoridades de Certificación o podrá, con su firma digital, autenticar o certificar documentos electrónicos en que la ley establezca el requisito de autenticación notarial.

En las legislaciones que han reconocido el uso de firma digital y en el proyecto de ley nacional se establece la conceptualización de la Firma Digital y la Firma Digital Avanzada.

Para nuestro Proyecto será "avanzada", la firma digital que es certificada por el organismo acreditador (prestador de servicios de certificación acreditado) , la cual tendrá el mismo valor jurídico que la firma manuscrita, siempre y cuando esté basada en un certificado digital reconocido y que haya sido producida por un dispositivo seguro de creación.[2]

---

[1] El Financiero #297 (Semanario), 29 de Enero –4 de Febrero del 2001, p. 21

[2] Proyecto de Ley de Firma Digital y Certificados Digitales, Op. Cit. artículos 2.12, 4 y 5. Es muy posible que al aprobarse el proyecto, este concepto de firma digital avanzada cambie a firma digital acreditada

Según lo establecido en el Proyecto para que opere el principio de equivalencia funcional de la firma digital y el principio de neutralidad tecnológica para los documentos electrónicos, será necesario que sean acompañados por un Certificado Digital.

Consideramos que para actos o transacciones comerciales electrónicas siempre debe tratarse de firma digital avanzada, pues la fuerza probatoria de una firma digital que no esté acompañada de un certificado digital estará sujeta a las reglas de la sana crítica, pues no puede hacerse valer su integridad y su autenticidad.

Solo la Firma Digital Avanzada será la que sirva para el cumplimiento de la finalidad perseguida por el sistema, quedando la firma no avanzada como un sistema residual que se utilizará para comunicaciones informales o para comunicaciones al interno de empresas, pues si se requiere certeza en cuanto a la vinculación de una declaración o mensaje de datos con su autor, se necesitará de una firma avanzada.[1]

[1] GONZALEZ –ECHENIQUE CASTELLANOS DE UBAO (Leopoldo). Estudios de la Directiva y del Decreto ley de 17 de Septiembre de 1999, sobre Firma Electrónica. Derecho de Internet, Contratación Electrónica y Firma Digital. España, Editorial Aranzadi S.A. 1ª. Edición, 2000, p. 222.

CAPÍTULO TERCERO

SUSTENTO DE LA FIRMA DIGITAL AVANZADA

SECCIÓN I: LOS CERTIFICADOS DIGITALES

A) Qué es un Certificado digital.

Los Certificados Digitales son documentos digitales o "registros electrónicos" firmados por una Autoridad de Certificación, que atestiguan que una clave pública corresponde a un individuo o entidad determinada, vinculando el certificado con la identidad del usuario.[1]

El autor Renato Jijena Leiva lo conceptualiza como "un documento digital emitido por una Tercera Parte Confiable que acredita o respalda la correspondencia entre una llave magnética y la persona que es titular de la misma, el que se añade a una firma electrónica como datos o información característica del firmante para acreditar su identidad digital."[2]

La principal función del Certificado es identificar el par de llaves con un usuario, de manera que quien pretende verificar una firma digital con la clave pública que surge de un Certificado, tenga la seguridad que la correspondiente clave privada es del firmante.

Con el Certificado se evita que otra persona utilice una clave o una combinación de ellas, asegurando en el sistema ser otra persona. Se alcanzan

---

[1] DEVOTO (Mauricio) El dinero Electrónico y el Lavado de Dinero. Op.cit.
[2] JIJENA LEIVA (Renato) Internet Certificada. www. acerita.com, Abril, 2001.

mayores grados de confianza, por cuanto el receptor de un mensaje puede tener plena seguridad que el emisor del mismo es quien dice ser y que éste a su vez, no puede negar o repudiar el envío.

Existen varias clases de Certificados, que vinculan la firma digital con la entidad y utilizan archivos digitales definidos por el estándar ITU X.509.[1]

Generalmente se establecen cuatro clases de Certificados, a saber:

1- En su forma más básica (clase uno) contendrán una clave pública y el nombre del firmante, el nombre de la autoridad de certificación, su correo electrónico y la clave pública de la entidad, la fecha de emisión y vencimiento de la clave, el número de serie del certificado y la firma digital del que otorga el certificado.[2]

2- Los Certificados de Autorización (clase dos) contienen más información del usuario, pues proveen información comercial, el lugar y puesto de trabajo, calificación de crédito o capital social en caso de ser una persona jurídica.

---

[1] AGUILAR SÁNCHEZ (Edwin) Seguridad y Privacidad en las Transacciones Digitales. Seminario de Notariado Digital, Registro Público, 2001, Documento sin numeración.

[2] Todas las legislaciones recogen el formato más difundido por las normas ISO sobre el tema, que también se realiza en nuestro Proyecto de Ley de Firma Digital y Certificados Digitales, agregando en el artículo 10 que se podrá exigir cualquier otro que el Reglamento se establezca.

3- En los casos de los certificados catalogados generalmente como clase tres, pueden determinar el día y la hora en que el documento fue firmado digitalmente (Digital time-stamp certificates).

4- También el Certificado clase cuatro puede atestiguar la existencia o validez de un determinado hecho o acto. Es con este certificado que se inicia el tema de las Autoridad de Certificación en el rol de notario.[1]

Es en este aparte donde debemos hacer una distinción en cuanto a las corrientes que consideración al sistema de Certificados Digitales como un notario electrónico y por tal invadiendo funciones delegadas por el Estado a los Notarios Públicos y otras que no lo consideran así.

Los que sostienen que no se transgrede las funciones Notariales indican que el Certificado Digital "es un instrumento de **Autenticación Digital** creado para establecer la confianza en las transacciones electrónicas **('trust')**."[2]

El M.Sc Edwin Aguilar subraya el término autenticación digital. La misma **no es una autenticación legal**, ya que no tiene que ver con la "Fe Pública", sino con

[1] RAMOS SUAREZ (Fernando) Como aplicar la Nueva Normativa sobre Firma Electrónica. www.publicaciones.derecho.org./redi. Documento sin numeración de página.
[2] AGUILAR SÁNCHEZ (Edwin) Reglas Generales para las Firmas, Certificados y Contratos Digitales. Seminario de Notariado Digital, Registro Público, 2001, Documento sin numeración.

la "Buena Fe" en las transacciones comerciales electrónicas que preserva su seguridad.[1]

Esta posición parece que tiene su fundamento en el hecho que cuando se requiere que un documento digital requiera autenticación legal mediante la firma de un Notario, será este quien estampe su firma digital. Por ejemplo en España el Real Decreto-Ley sobre Firma electrónica reconoce que la Firma Electrónica no equipara al documento electrónico con el instrumento público, para lo que se requiere la intervención de un Fedatario Público, quien firmará el documento con su firma digital avanzada[2].

Esta es la posición predominante ya que existe una Directiva del Parlamento Europeo y del Consejo para los Estados miembros de la Comunidad Europea, que establece que pueden mantener restricciones a los contratos que requieran por ley, para surtir efectos rente a terceros, la certificación o la fe pública notarial, distinguiendo que no hay invasión de competencia entre las Autoridades de Certificación y la actividad notarial.[3]

Por otro lado está la corriente que considera que cuando las Autoridades de Certificación autentican a las partes en el sistema, estarían ejerciendo la potestad

---

[1] Exposición del M.Sc. Edwin Aguilar Sánchez en el Seminario de Notariado Digital en el Registro Público.
[2] GONZALEZ –ECHENIQUE CASTELLANOS DE UBAO (Leopoldo) Op.Cit. p. 223. En costa Rica el Proyecto de Ley sobre Firmas Digitales y Certificados Digitales también lo establece en el artículo 6.
[3] Directiva del Parlamento Europeo y del Consejo 2000/31/CE del 8 de Junio del 2000.

jurídica de otorgar fe pública en el marco de las transacciones comerciales electrónicas.[1] Si se sigue esta corriente, consideramos indispensable la intervención del Notario Público como parte fundamental de la Autoridad de Certificación en la fase de creación de la firma digital, pero también sería necesaria su participación para que los documentos se eleven a la calidad de instrumentos públicos.

En este punto es interesante lo resuelto por el Tribunal Constitucional de Colombia, [2] en cuanto a la "fe pública y la función notarial".

La demanda de inconstitucionalidad fue promovida por un grupo de Notarios, contra la Ley 527 del 18 de Agosto de 1999, mediante la cual se reglamentan los mensajes de datos, el comercio electrónico y la firma digital. El argumento principal de los quejosos era que las funciones de las entidades de certificación estarían dando "fe pública" en Colombia, cuando esta función esta reservada constitucionalmente de manera exclusiva a los Notarios.

La Corte constitucional de Colombia señaló que "las entidades de certificación certifican técnicamente que un mensaje de datos cumple con los elementos esenciales para considerarlo como tal, a saber la confidencialidad, la

---

[1] JIJENA LEIVA (Renato) Internet Certificado. Op.cit.

[2] MUÑOZ ESQUIVEL (Oliver) Actividad de las Entidades de Certificación frente a la Función Notarial, www.pulbicacionesderecho.org/redi, #25 15 de Junio , 2000, documento sin numeración de páginas, citando la Sentencia C-662-00 del Tribunal constitucional de Colombia del 08 de Junio del 2000.

autenticidad, la integridad y lo no repudiación de la información, lo que, en últimas permite inequívocamente tenerlo como auténtico." [1]

Finalmente la Corte Constitucional concluyó que "si bien el carácter eminentemente técnico de su función es indiscutible, la misma participa de un importante componente de la tradicional función fedal, pues al igual que ella, involucra la protección de la confianza que la comunidad deposita en el empleo de los medios electrónicos de comunicación", señalando además que el hecho de que la función pública fedante haya sido investida en los notarios por mandato constitucional, no significa que la misma constituye una función constitucional privativa y excluyente.[2]

Como vemos la Corte Constitucional Colombiana reconoce la semejanza de la función de las Entidades de Certificación con la función Notarial, destacando su importante contenido técnico, lo cual da la confianza necesaria para incentivar el desarrollo progresivo de las vías electrónicas de comunicación.

En cuanto a esta discusión debemos estar claros que solamente mediante una ley, se puede depositar la función de la "Fe Pública" en las Autoridades de Certificación. No es posible pensar que solamente por autenticar a las personas en el sistema, estarán ejerciendo funciones propias que la ley no les otorga.

---

[1] MUÑOZ ESQUIVEL (Oliver) Op.cit.
[2]MUÑOZ ESQUIVEL (Oliver) Op.cit.

Por esta labor de emisión de certificados digitales, las Autoridades deben ser entes fiables y ampliamente reconocidos pues confirman las claves públicas de los usuarios, rubricando con su propia firma la identidad del usuario, responsabilizándose legalmente por dicha identificación.

Para que una persona física o jurídica obtenga su firma digital y su certificado digital, será necesario que realice su solicitud ante un Agente Certificador, quien verificará la documentación (cédula de identidad, estatutos societarios o certificaciones de personería o cualquier otro documento de identificación necesario) y dará fe de la identidad del usuario, por lo que será necesario que dicho Agente sea Notario Público[1].

Con la intervención de un Notario se cumpliría con la función de protección a los derechos fundamentales de las personas físicas en cuanto a su intimidad, porque se garantizaría el tratamiento adecuado, desde el inicio, de los datos personales del usuario.[2]

---

[1] El sitio web www.acertia.como, en su artículo sobre El rol del Fedatario, indica que en la clasificación de los Certificados en México existen tres niveles, dependiendo de la información que contengan, siendo el del nivel 3 el de mayor valor y alcance por la intervención de un Fedatario Público en el proceso de emisión del certificado y por la fe pública aplicada en ellos.

[2] Esta garantía esta contemplada en las legislaciones modelo y en la Directiva Europea del 24 de Octubre de 1995, sobre la Protección de las personas físicas en cuanto a sus datos y su libre circulación. VeriSign una de las empresas más conocidas que brinda servicios de certificación, emite electrónicamente los certificados que le son solicitados, pero cuando se le solicita un certificado de clase 3, los usuarios deben concurrir personalmente ante un Local Registration Authority o un delegado que será un Notario.

Como hemos observado el Notario Público tiene un nuevo campo donde desarrollar su función fedal, que debe conjuntarse con la labor de las Autoridades de Certificación para trasladar la fe pública al campo virtual, como veremos en el desarrollo del tema del Notario Cibernético.

Consideramos que no debemos confundir las funciones que realizan los Notarios y las Entidades de Certificación, aunque ambas tengan la finalidad similar de dar seguridad: uno da seguridad jurídica y otro seguridad tecnológica.

La función notarial seguirá conservando particular relevancia con respecto a los actos o negocios jurídicos que requieren para su validez y eficacia la autorización de un Notario Público, complementando, además, las labores que realizan las Entidades de Certificación. Como estableció acertadamente la Corte Constitucional Colombiana, será únicamente mediante la promulgación de una ley, que se pueda depositar la función de la fe pública en las Autoridades de Certificación, por lo que no existiendo dicha ley, la función es propia de los Notarios Públicos.

Verificado lo anterior y obtenido el software, se genera el Certificado Digital del solicitante y lo registra ante la Autoridad que corresponda.

B) Registro de Certificados Digitales.

Los Certificados se inscriben en un Registro o "Repository", que son la base de datos a la que el público puede acceder on-line, para conocer la validez de los certificados o cualquier otra circunstancia relacionada con ellos, como serían los certificados suspendidos o revocados por las autoridades certificantes acreditadas, así como los extravíos o robos de claves privadas.

Los Certificados tienen un duración limitada, "pero una serie de circunstancias, entre la que destaca la de que exista el peligro de que la clave privada sea conocida por un tercero, hacen que sea preciso que los certificados puedan revocarse anticipadamente, de forma que una vez efectuada la publicación de la revocación se destruya la apariencia creada por la difusión y el empleo de la clave pública en el tráfico y no se responda ya con base en ella"[1].

Para que un Repository sea reconocido debe operar bajo la dirección de una Autoridad Certificante Acreditada, que será el proveedor de los servicios de certificación. Esto quiere decir que la eficacia jurídica de la firma digital tendrá como condición sine qua non, la intervención en el proceso de las terceras partes de confianza o TTP (Trusted Third Parties).[2]

---

[1] ALONSO UREBA (Alberto) ALCOVER GARAU (Guillermo) La Firma Electrónica. Derecho de Internet, Contratación Electrónica y Firma Digital. España, Editorial Aranzadi S.A. 1ª. Edición, 2000, p. 186.
[2] RAMOS SUAREZ (Fernando) Como aplicar la nueva normativa sobre la firma Electrónica. www.legalia.com Documento sin numeración de página.

Para dar mayor seguridad jurídica a la firma electrónica, el notario publico debe tener un papel importante y ser parte de la red de certificación digital, ya que será la persona que se cerciorará de la identificación del titular del certificado antes de proporcionar la firma electrónica, como lo haríamos en el caso de la contratación tradicional y además cuando la ley exija que el documento electrónico este certificado o autenticado por un abogado o notario, este requisito se cumplirá con la firma avanzada del Notario. La ley italiana sobre creación, almacenamiento y transmisión de documentos en forma computarizada o por sistemas telemáticos del 10 de Noviembre de 1997, dispone que el Notario puede autenticar un firma digital certificando que fue puesta en su presencia y que el documento firmado refleja la voluntad del signatario, sustituyendo cualquier sello, marca o signo distintivo que se requiera.[1]

Diferentes legislaciones han incluido normas relativas a los Certificados Digitales, para que cumplan su labor con plena validez legal. En este punto será necesario que la ley nacional o su reglamento sin ninguna duda determine:

> Enunciar los requisitos de normalización de acuerdo a estándares internacionales.

---

[1] RUIZ-GALLARDON (Miguel) Fe Pública y Contratación Telemática. Derecho de Internet. Contratación electrónica y firma digital. . España, Editorial Aranzadi S.A. 1ª. Edición, 2000, p. 116

- Las condiciones de vigencia de los certificados, a fin de determinar su emisión, aceptación, revocación, suspensión y expiración.
- Establecer los derechos y obligaciones del suscriptor y de la Autoridad Certificante emisora.
- Establecer los requisitos de publicación de los certificados y de las listas de certificados revocados y suspendidos.

Estos son requisitos que la mayoría de las normativas internacionales han ido adoptando por su necesidad. Son recomendadas por las legislaciones modelo sobre firma digital y por organismos como el Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la ABA de los Estados Unidos.

Como vemos, la firma electrónica da lugar a una gran variedad de nuevos servicios y productos relacionados con ella o que la utilicen. La definición de dichos productos no deben limitarse a la expedición y gestión de certificados, sino incluir también cualquier otro servicio o producto como los de Registro, de estampado de fecha y hora, los servicios de guías de usuarios, las de cálculo y asesoría relacionados con la firma.[1]

[1] Exposición de motivos de la Directiva del Parlamento Europeo y del Consejo 1999/93/CE del 13 de diciembre de 1999, en la que se establece un marco comunitario para la firma electrónica.

SECCIÓN II: LAS AUTORIDADES CERTIFICADORAS

A) Quienes son las Autoridades Certificadoras.

El sistema de criptografía asimétrica requiere que un tercero certifique el resumen que dará origen a la firma digital. Esta tercera parte produce, distribuye y controla las firmas digitales y se les conoce generalmente como AUTORIDAD CERTIFICADORA (nombre emanado del empleado en el derecho sajón norteamericano: Certificatión Authority).

Las Autoridades Certificadoras son las encargadas de emitir los Certificados Digitales que dan certeza y seguridad a los documentos o mensajes firmados digitalmente.

Estas Entidades se han convertido en una base importante para el comercio electrónico, pues permiten verificar la existencia de un acto electrónico, identificar a las partes intervinientes en un contrato y evitar que se den errores por falta de personería jurídica.

Con el nacimiento de las Autoridades de Certificación se solucionaron los problemas de anonimato, firmas, identificación y falta de seriedad en el cumplimiento de los contratos.

"A partir del momento en que comenzó a aplicarse la autenticación muchas de estas cuestiones es obviaron, ya que las partes quedaban lo suficientemente individualizadas como para sentir que deberían responder tanto civil como penalmente e sus actividades cibernéticas, por lo que evidentemente la autenticación comenzó a prestar un servicio invaluable al desarrollo del comercio a través del sistema EDI."[1]

No nos extenderemos en el análisis de esta institución, ya que hemos ido tratándolas en el desarrollo de la investigación, por lo que veremos sus generalidades para ser autorizadas como tal.

Estas instituciones técnicas proveen seguridad, basado en la confianza y honorabilidad que ellas garantizan.

B) Funciones de la Autoridades de Certificación.

Para complementar el conocimiento de quienes son estas Autoridades debemos determinar qué funciones cumplen.

Sus principales funciones se pueden resumir en:

1- Expedir y revocar certificados digitales.

[1] GAETE GONZALEZ (Eugenio) Firma Electrónica y Firma Digital. Op.cit. p. 12

2- Crear y publicar las listas de revocación, extravío o robo de claves, por lo que si se envía un documento firmado digitalmente que ha sido revocado, la firma es inválida. Debe cumplir como una Autoridad de Registro donde se verifican la identidad del firmante, dando la seguridad al sistema.

3- Base de datos de Certificados en donde se da el almacenamiento y acceso de listas de usuarios, certificados y listas de revocación de certificados. Las Autoridades de Certificación deben garantizar rapidez y seguridad en la rapidez del servicio de consulta a sus Registro.

4- Administración y seguridad de claves, que funciona como un depósito de claves.

5- Emisión de Certificados de Estampado Cronológico (Time Stamping)

6- Certificación validada por políticas y restricciones en toda la cadena de certificación, o sea que debe tener una pirámide de seguridad que valide la certificación.

7- Deben tener un servicio de recuperación de claves para el evento de daño de los discos duros.[1]

[1] AGUILAR SÁNCHEZ (Edwin) Seguridad y Privacidad en las Transacciones Digitales. Op.cit.

Por la creciente participación de los negocios por medios electrónicos, es indispensable una adecuada regulación de las entidades de certificación, pues es necesario establecer una estructura que brinde confianza a las transacciones, no solo desde el punto vista técnico, sino también jurídico.

Aunque el nombre de "Autoridad de Certificación" tiene una connotación de ente público, estas pueden ser públicas, a través de un organismo estatal, o privadas pero bajo la supervisión de una entidad Estatal porque su actividad se debe someter a los principios del derecho público.[1]

En Costa Rica el Proyecto establece un régimen abierto, ya que pueden ser empresas públicas o privadas, las cuales deberán someterse al proceso de acreditación ante una Autoridad adscrita al Ministerio de Ciencia y Tecnológica, quien fungirá como Órgano Rector (Art. 9).

Consideramos que este régimen es el mejor ya que los usuarios podrán certificarse con una institución publica que podrá emitir certificados para su contribuyentes con bajo costo para sus relaciones administrativas, las cuales

[1] En Europa y de conformidad con la Directiva 1999/93/CE del 13 de Diciembre de 1999, los servicios de certificación pueden ser prestados, tanto por entidades públicas como por personas físicas o jurídicas, cuando así se establezca de acuerdo con el derecho nacional

podrán ser utilizados para otros actos siempre y cuando no caigan en competencia desleal con los certificados expedidos por la empresa privada.[1]

Por ser diferente el animo de la función de las Autoridades en el sistema de los Estados Unidos, indicamos cuales han sido los dos enfoques que han predominado en dicho sistema: el primero los concibe plenamente regulados por el Estado (Utah y Washington) ; los segundos estiman que tal labor no le corresponde al Estado, sino que su regulación debe quedar en manos de la empresa privada, siendo por ende tales estatutos totalmente abiertos.

Lo que si es preciso es que no importando si son empresas privados o públicas, será necesario que cumplan con los requisitos legales que garanticen la seguridad de los usuarios.

Las funciones de las Autoridades de Certificación tienen mucha relación con sus deberes, por los cuales se proporciona un medio de acceso que permitan a la parte determinar mediante el Certificado Digital:

a) la identidad de la Autoridad Certificadora;
b) Que el método utilizado para identificar al firmante que tiene su clave privada y que la misma está vigente; y
c) Que el firmante tiene bajo su control los datos de creación de la firma.

---

[1] BARZALLO (José Luis) Ecuador: Los Terceros de Confianza en el Comercio Electrónico. Revista Electrónica de Derecho Informático, #33, www. publicacionesderecho. Org/redi. Abril, 2001.

d) Que los datos de creación de la firma eran válidos, por lo que el certificado es válido.

e) El deber más importante es utilizar sistemas, procedimientos y recursos humanos fiables, de manera que se guarde la confidencialidad y custodia de los documentos e información entregada por los usuarios.[1]

Estas funciones y deberes de las Autoridades Certificadoras regularmente no están reguladas mediante ley, sino que es normal encontrar sus disposiciones de manera reglamentaria.[2]

Mientras las firma digital soluciona el problema de la verificación dando la seguridad de la no falsificación del mensaje, la Autoridad Certificadora resuelve el problema de la autenticación de las partes.

C) Requisitos de las Autoridades de Certificación.

Como es de esperar, no cualquiera puede ser una Autoridad Certificadora, sino que tienen que cumplir con una serie de requisitos para ser acreditada y

---

[1] AGUILAR SÁNCHEZ (Edwin) Reglas Generales para las firmas, Certificados y Contratos Digitales. Seminario de Notariado Digital, Registro Público, 2001, documento sin numeración. La Directiva del Parlamento Europeo y del Consejo del 24 de Octubre de 1995, sobre el tratamiento de datos personales y su libre circulación, establece el derecho de acceso del interesado a los datos que las Autoridades de Certificación tienen, su oposición y a la seguridad de dichos actos.

[2] En España las obligaciones de los prestadores de servicios de certificación fue regulada mediante Reglamento elaborado por el Ministerio de Fomento por Orden del 21 de Febrero del 2000.

reconocida legalmente como una organización competente para llevar a cabo tales funciones.

Las Autoridades Certificadoras deben someterse a un proceso de acreditación para ser debidamente acreditados. En Costa Rica el Proyecto de Ley de Firma Digital y Certificados Digitales establece que la acreditación la realizará una Autoridad adscrita el Ministerio de Ciencia y Tecnología. [1]

Los requisitos que normalmente se exigen deben ser adaptados al sistema jurídico, basados en estándares internacionales mínimos sin los cuales la función de certificación pierde su valor.

En doctrina estos requisitos para considerar a una entidad de certificación, se pueden enumerar así:

1- Contar con capacidad económica y financiera suficiente para prestar los servicios de certificación digital y responder por los riesgos de su función.

Las Autoridades de Certificación deben disponer de recursos económicos suficientes para operar y afrontar el riesgo de responsabilidades por incumplimiento de sus funciones y por los daños y perjuicios que ocasionen. "La

[1] Proyecto de Ley de Firma Digital y Certificados Digitales, Op.Cit., artículo 13.

garantía podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un seguro de caución."[1]

La capacidad económica es imprescindible porque pueden darse eventos externos como un corte de energía eléctrica o interno como negligencia de los funcionarios de la Entidad, que hagan imposible la correlación de llaves públicas, en la publicación de las revocaciones o que se entorpezca el servicio de generación de llaves y su almacenamiento[2].

2- Contar con capacidad tecnológica para sus funciones, garantizando el cumplimiento de los estándares de seguridad, privacidad y auditoria.

Debe existir una pirámide de seguridad, por el cual se crea un ambiente seguro, que debe tener:

a) Políticas y Procedimientos que establezcan estándares para el manejo de la seguridad en todo el sistema;
b) Autenticación fuerte que controla los accesos y certifique (no repudio) o rastrea las acciones de los que ingresan al sistema;
c) Autorización a los usuarios para que accedan a las áreas apropiadas una vez que cuando lo autentica;

---

[1] ALONSO UREBA (Alberto) La Firma Electrónica. Derecho de Internet. Contratación electrónica y firma digital. . España, Editorial Aranzadi S.A. 1ª. Edición, 2000, p. 197.
[2] GONZALEZ –ECHENIQUE CASTELLANOS DE UBAO (Leopoldo) Op.Cit. p. 240.

d) La encripción que proteja los datos de ser husmeados (confidencialidad) y alterados (tampering); y

e) Una auditoría que chequea y confirma la eficacia de las políticas, los procesos y las acciones individuales. [1]

3- Contar con políticas y procedimientos de seguridad en toda la cadena de creación de certificados, bajo el régimen de responsabilidad que se le aplique. Se inicia con la Autoridad de Registro, que constata la información del suscriptor.

4- Los representantes legales, directores y administrados no deben haber sido condenados a prisión, ni suspendidos o excluidos del ejercicio de su profesión. Este punto es muy lógico por los deberes de confidencialidad y custodia de la información de los usuarios, de manera que dicha información no sea "vendida" para otros efectos. [2]

Con el cumplimiento de estos requisitos mínimos, las entidades de certificación pueden funcionar y emitir los certificados que sean requeridos por sus clientes. Asimismo implica que todos los certificados emitidos por ellos serán válidos y pueden hacerse valer en estrados judiciales.

---

[1] AGUILAR SÁNCHEZ (Edwin) Seguridad y Privacidad en las Transacciones Digitales. Op.cit.
[2] AGUILAR SÁNCHEZ (Edwin) Reglas Generales para las Firmas, Certificados y Contratos Digitales. Op.cit.

En cuanto a las Autoridades de Certificación, consideramos que habrá que determinar mediante inclusión en el proyecto de ley nacional de firmas digitales y certificados digitales o en su reglamento lo siguiente:

- Los requisitos para actuar como Autoridad de Certificación.
- Las causales de revocación o suspensión de su licencia.
- Establecer en todos los casos la publicidad de sus procedimientos, de manera que se permita su conocimiento por terceros.
- Establecer las bases de control a través de auditorias, a fin de evaluar su gestión.
- Determinar los alcances de la responsabilidad de las partes, incluyendo la de las Autoridades Certificadoras.

Existe muchas experiencias en otras legislaciones de la cual nos podemos valer para incluir en nuestra normativa, a efecto de que sea más homogénea con la normativa internacional, sin peder de vista la realidad nacional.

Como vemos el tema de las Autoridades de Certificación es importante para la concepción de la contratación electrónica notarial, el instrumento público electrónico y la concepción del Notario Cibernético como parte de todo el sistema de certificación electrónica.

TÍTULO CUARTO

EL NOTARIO CIBERNÉTICO

CAPÍTULO PRIMERO

LA FIGURA JURÍDICA DEL NOTARIO CIBERNÉTICO

SECCIÓN I: NACIMIENTO DE LA FIGURA (Common Law)

La idea de crear un profesional que realizara la labor notarial en un ámbito cada días más desarrollado como es la electrónica, surge en los Estados Unidos de América.

En Agosto de 1994 se marca una nueva era para la profesión notarial, cuando por recomendación del Comité de Seguridad de Información (Informatión Security Committee) de la Sección de Ciencia y Tecnología, la "American Bar Association" (ABA) acordó una resolución para colaborar con cualquier otra organización nacional o internacional en el propósito de lograr una especial certificación de los Notarios Ciberneticos.[1]

El Presidente del "Cybernotary Comittee" de la ABA, Ted Barassi, entregó el 30 de Abril de 1996, un proyecto de ley a través del cual se pretendía introducir la figura del "Ciber-Notario". El señor Barassi compuso un breve tratado sobre la ignorada y amplia actividad del notario en su significación latina y las razones en

[1] KENNAIR (William B.) El Concepto y Desarrollo del "Cybernotary" en Boletín de la Comisión de Asuntos Americanos, Unión Internacional del Notariado Latino, República Dominicana, Año VII,N°27, Febrero de 1998, p.8

las que se basa la necesidad de la creación de una adecuada categoría profesional en los Estados Unidos.[1]

Esta figura del Ciber-Notario, más relacionada con la concepción del notariado latino, responde a la necesidad real y urgente de proveer seguridad jurídica a las transacciones internacionales realizadas por medios electrónicos ante el nuevo mercado de la globalización que significaba un mercado sin fronteras. Constituye en el primer acercamiento de la profesión notarial con la electrónica y el intercambio de datos que se deriva de ella.[2]

Los Abogados americanos sintieron que se debía buscar un mecanismo híbrido con el del notariado latino, a efecto de que los documentos originados en los Estados Unidos no fueran rechazados por las autoridades legales o registrales del exterior, obligándose a los contratantes a buscar asesoramiento legal en los países donde querían hacer valer dichos contratos.

Es por ello que, además de esa necesidad de proveer seguridad jurídica mediante la certificación y autenticación de dichas transacciones internacionales vía computadora, se requería demostrar la validez en cualquier jurisdicción de dichas transacciones, sin adicionarle costos excesivos.

---

[1] Nacimiento del Ciber-Notario. Revista Internacional de Notariado, N° 94, ONPI,Buenos Aires, Segundo Semestre, año 1997, p-104., extracto de la Revista NOTA BENE del 22 de Agosto de 1996.
[2] MARRERO (Angel R.) El Notario Cibernético. Boletín Informativo de la Asociación de Notarios de Puerto Rico ANOTA, Año 9, N° 2, Abril-Mayo de 1995, p. 4.

La concepción del Cibernotario rompe con la concepción tradicional del notariado en el Common Law, aplicando concepciones propias del sistema latino.

Es por ello que dicho profesional sería un abogado especialista en servicios relacionados con la certificación de transacciones y documentos internacionales realizados electrónicamente, que asesora a las personas que le soliciten sus servicios. Estaría en capacidad para redactar documentos en forma legal con plena validez, así como de autenticar los actos y contratos que las partes otorguen.

Con los Cibernotarios, la ABA pretendía llevar a su sistema de common law, la especialidad jurídica que llena satisfactoriamente las necesidades de competencia profesional y seguridad que tiene el sistema de notariado latino. En el sistema latino los notarios son responsables de crear y diseñar los documentos con validez legal y obligatoriedad para las partes que intervienen en ese acto.

Es por esa distinción que los notarios americanos para llegar a ser cibernéticos, se convierten en una figura desconocida en su sistema ya que serán responsables por los actos autenticados por ellos.[1]

Este sistema equipara la validez de certificación de dichos notarios, con la validez de los actos realizados en el sistema latino, elevando el nivel de la profesión notarial en los Estados Unidos.

---

[1] KENNAIR (William B.) Op.cit., p. 8

Con la resolución adoptada por la ABA, el Comité de Seguridad e Información propuso varios puntos importantes para la implementación de la iniciativa de los cibernotarios. Estos puntos son:

a) La creación de un cuerpo auténticamente con fe pública, capaz de diligenciar y administrar la profesión, junto con la preparación y calificación de criterios, incluyendo los requisitos de conocimientos técnicos.

Los Cibernotarios serían Notarios Públicos regidos por las leyes estatales aplicables en los Estados Unidos, por lo que deben obtener la licencia de Notario en el propio Estado de pertenencia para poder gozar de la autoridad para certificar conferida a los Notarios Públicos; luego tendrían que aprobar los exámenes de admisión para la especialización según el programa establecido por el Comité Directivo de la ABA.[1]

"Cybernotary" se desarrolla en Estados Unidos con el esfuerzo conjunto de el Comité de Seguridad e Información de la ABA, el Consejo Estadounidense para Negocios Internacionales (USCIB) y el Banker's Trust, quien desde su inicio hizo aportes fundamentales con el apoyo de su red electrónica de comercio. [2]

---

[1] MICCOLI (Mario) Cybernotary. Revista Internacional de Notariado Latino. N°91, primer semestre, 1996, p.135. Estos exámenes incluyen la comprensión del sistema de firma digital y como evitar su alteración y falsificación.

[2] Cybernotary fue una marca registrada a cargo del Banker's Trust por cuenta de la American Bar Association hasta que se estableció el CyberNotary Committee.

b) La creación de una legislación para lograr una equivalencia con el sistema latino, en cuanto a práctica y autenticidad.

Además del valor de la autenticación, muchas operaciones requieren de una seria asesoría legal y seguridad jurídica, por lo que se requiere que el especialista estuviese dotado de la cultura jurídica propia de un abogado al igual que en nuestro sistema de notariado.

Como la función del Notario Cibernético incluye la combinación de funciones de notario y abogado, "en toda transacción internacional realizada electrónicamente el Notario Cibernético deberá asegurarse sobre:

1- Identidad de las partes;
2- La capacidad de las partes y de sus representantes para negociar y llevar a cabo la transacción;
3- El propósito e intención de la transacción;
4- La autonomía y la libertad de las actuaciones de las partes;
5- La disponibilidad del objeto de la transacción;
6- La conformidad del lenguaje contractual con la intención de las partes; y
7- La legalidad del propósito e intención de las partes con las disposiciones de ley aplicables."[1]

[1] MARRERO (Angel R.). Op.cit. p. 4.

Como vemos realizará una función que para los Notarios del sistema latino es propia de la función misma.

c) La acreditación, reconocimiento y aceptación que permitan la oponibilidad frente a terceros de los actos de los cibernotarios.[1]

El desarrollo del reconocimiento de la firma digital y en énfasis en la creación de servicios de terceras partes confiables, son esfuerzos importantes realizados en los Estados Unidos para dar la investidura necesaria a los Notarios que trabajen en comercio electrónico.

El reconocimiento del Cibernotario como una tercera parte confiable hace que su actuación goce de validez y sea oponible, por cuanto será un experto en sistemas de seguridad informativa y tecnológica, que podrá certificar electrónicamente y dar autenticidad a todos los elementos electrónicos en una operación comercial (Legalización electrónica de firmas digitales).[2]

El documento notarial cibernético gozará de presunción de legalidad y certeza. La presunción de legalidad significará que el acto contenido en el documento cumple con los requisitos legales necesarios para su validez, pues las partes contratantes han prestado su consentimiento libre e inteligente, y que los hechos y términos expresados en el documento son correctos.

---

[1] KENNAIR (William B). Opcit., p. 11.
[2] Ibid.

El Notario Cibernético proveerá un alto nivel de seguridad, ya que será el responsable del contenido de los términos del mensaje, con la hora y fecha de la intervención notarial.

Aunque para muchos el tema pareciera de ciencia ficción, los avances de la era informática y del comercio electrónico en un mercado globalizado, hacen que esta idea esté cada vez más cercana a las necesidades de nuestra sociedad.[1]

Como expusimos, la figura de este profesional nace en los Estados Unidos, por lo que varios Estados han desarrollado e implementado legislación sobre firma digital entre ellos Florida, Arizona, Georgia, Hawai, Oregon, Washington, Illinois y California.[2]

En ausencia de una Ley modelo, el primer Estado que implementó el uso de la firma digital como Ley, fue el Estado de Utah, (Utah Digital Signature Act, que comenzó a regir el 1 de Mayo de 1995) por cuya razón se ha convertido en referencia obligatoria para los demás Estados de la Unión Americana. Posteriormente la Sección de Ciencia y Tecnología de la ABA publicó la Guía de

---

[1] Aún en 1999 en la Ciudad de los Angeles, en el sitio web de Los Angeles County Bar Association, un artículo del señor Joseph Kornowski sobre el tema se titulaba "The Specter of the CiberNotary: Science Fiction or New Legal Speciality? www.lacba.org/lalawyer/tech/notary.

[2] DEVOTO (Mauricio). El Dinero Electrónico y el Lavado de Dinero. Revista Electrónica de Derecho Informático, Agosto, 1998. **www.publicaciones.derecho.org**. documento sin numeración de página.

Firma Digital, (Digital Signature Guidelines) que también ha servido modelo a las legislaciones de los Estados.[1]

Finalmente y como respuesta a los cambios operados en las comunicaciones entre las partes (socios comerciales) que recurren a las modernas técnicas informáticas y para armonizar el derecho mercantil internacional que impulsara el comercio internacional, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, aprueba la Ley Modelo de la CNUDMI para el Comercio Electrónico. Esta ley fue aprobada en la 85ª. Sesión plenaria de las Naciones Unidas, el 16 de diciembre de 1996.[2]

A partir de esos movimientos la idea ha ido tomando fuerza en el mundo, así vemos que en España se estableció mediante el Real Decreto-Ley 14/1999, sobre Firma Electrónica; en Italia, Inglaterra, Alemania y Holanda se ha hecho lo propio.

No debemos creer que en todos estos países en que el tema avanza, todas las fuerzas han estado de acuerdo, ya que por ejemplo en Holanda cuando en Octubre de 1996 se presentó a la Real Cofradía Notarial el informe preliminar sobre "El Notario y el acuerdo jurídico electrónico", el Lic. W.G Huijgen, Profesor de Derecho Notarial de la Universidad de Leyden, Holanda, presentó un informe personal donde indicaba que cuando el acuerdo jurídico necesita de la intervención

---

[1] Ibid.
[2] Ley Modelo de la CNUDMI sobre Comercio Electrónico, en www.uncitral.org

del Notario para su validez (escritura pública), dicha actividad no es compatible con la documentación electrónica en sí y que el advenimiento electrónico solo podría utilizarse para documentos privados y para efectos del Registro de la Propiedad y Registro Mercantil en su gestión notarial y no en el acto mismo. [1]

SECCIÓN II: LA FIGURA EN EL SISTEMA NOTARIAL LATINO

En nuestro continente los países que siguen el sistema Notarial Latino, que más han avanzado en el tema del reconocimiento del Documento Electrónico, la Firma Digital y el Certificado Digital son México, Colombia, Venezuela, Argentina, Chile y Perú, que están basados en la Ley del Estado de UTAH sobre Firma Digital, en la guía de Firma Digital de la ABA y en la Ley Modelo de la CNUDMI sobre Comercio Electrónico.[2]

Conforme transcurre el avance en la tecnología de la información, cada vez más países toman interés en el tema y se dirigen a su reconocimiento legal.

---

[1] KEMPER (Ana María) Seguridad Jurídica en la Contratación por medios electrónicos. Boletín Informativo de la Asociación de Notarios de Puerto Rico, ANOTA, Año 11, N°3, Junio-Julio, 1997, p. 9. También hay una reseña en: Informe de la K.N.B. sobre "El Notario y el acuerdo jurídica electrónico en Holanda", en Revista Internacional del Notariado, N°93, Primer Semestre, 1997, pp 136-139.

[2] IRIARTE AHON (Erick) Firma Digital y Certificado Digital. El Proyecto Peruano. Revista Electrónica de Derecho Informático. **www.publicaciones.derecho.org, p**. 1 La Ley de Firmas y Certificados Digitales del Perú, fue publicado en el Diario Oficial El Peruano, el 28 de Mayo del año 2000.

En nuestro país se están dando pasos hacia el reconocimiento de efectos jurídicos a los mensajes de datos electrónicos, con la presentación por parte del Ministerio de Ciencia y Tecnología del Proyecto de Ley en que se pretende otorgar validez legal a los documentos digitales,[1] al cual nos hemos referido en el desarrollo de la firma digital, los certificados digitales y seguiremos refiriéndonos.

Estando a las puertas de que nuestra legislación reconozca la Firma Digital y los Certificados Digitales, es importante visualizar qué se pretende en cuanto a la figura del Notario Cibernético en nuestros países de Sistema Latino.

La aprobación de estas leyes que reconocen la aplicación de la informática para la firma de documentos, no es más que un paso más del avance de la tecnología en los diversos campos de la sociedad y el campo del derecho no puede escapar a ello.

Diariamente en el campo del Derecho, los profesionales de la función notarial tenemos contacto con la informática por dos aspectos: primero porque el derecho en sí, es uno de los campos donde la ingeniería informática se ha abocado a la elaboración de programas que sean de utilidad en su labor diaria. Actualmente no existe una oficina donde los sistemas de cómputo no ayuden a realizar la labor de

[1] Proyecto de Ley de Firma Digital y Certificados Digitales, del 22 de Febrero del 2001, Expediente N° 14276 de la Asamblea Legislativa, que pasó a estudio e informe de la Comisión Especial de Propiedad Intelectual.

manera más rápida y eficiente, tanto en la información que se nos envíe como la que enviamos y la preparación de los instrumentos públicos.

El segundo aspecto de contacto se da porque es constante la utilización de soportes magnéticos para recibir y guardar información en las Oficinas Públicas que son requeridas para ejercer la función notarial (Por ejemplo el acceso al las diferentes Secciones del Registro Público vía Internet). Sin dejar de lado que una gran parte de la actividad documental en el comercio actual se desarrolla en forma automatizada.

Es por ello que estando en este mundo donde la tecnología de la información avanza en todas las esferas del quehacer humano y siendo el derecho una ciencia que se ocupa de los cambios sociales, no podemos cerrar los ojos a lo que acontece, sino que debemos replantear los conceptos con que se ha trabajado y analizar cómo podemos aplicar en nuestro campo estas nuevas formas de comunicación.

Los Notarios del Sistema Latino realizan las funciones que los del Sistema Notarial del Common Law quieren realizar, por lo que la implementación de un Notario Cibernético en nuestros países responde a necesidades diferentes.

Aún en los países del Sistema Latino, la necesidad de implementar esta figura, ante el avance de la tecnología, varía y será más acentuada tomando en

cuenta los requisitos para ser Notario y la jurisdicción territorial que se establece en las distintas legislaciones.

Hemos abordado la preocupación nacida en algún sector de la profesión notarial, que teme que los sistemas de seguridad empleados para el comercio electrónico (Certificados Digitales emitidos por las Autoridades de Certificación) puedan desplazar a los Notarios Públicos y, en los países que lo permiten, a los Corredores en su función de Fedatarios Públicos.

Esta posición se da un poco por el desconocimiento del tema y también por el poco conocimiento del mismo. Decimos que por el poco conocimiento, porque es muy posible que estén fundadas en lo acontecido en los Estados Unidos, en donde las Autoridades Certificadoras han venido a reemplazar al Notary Public.

Pero este desplazamiento de los Notary Public norteamericanos se debe a que estos no tienen dentro de sus funciones contempladas por ley, la de autenticar firmas digitales y las funciones propias del notario latino. Esta posición ha ido cediendo terreno por cuanto con el paso del tiempo y la experiencia lograda, la función autenticadora le está siendo entregada en algunos casos a los Notarios, que es en donde nuestro sistema la tiene depositada por ley.[1]

---

[1] GAETE GONZALEZ (Eugenio) La Firma Electrónica y la Firma Digital. Op.cit. p. 13 Recordemos el caso de Verisign citado que cuando se le solicita un certificado clase tres, requiere la intervención notarial.

Nuestra posición en cuanto a este punto fue externada supra en la Sección de Certificados Digitales, en cuanto los sistemas de seguridad que se logran con la firma digital y los certificados digitales otorgan una autenticación digital (buena fe y seguridad tecnológica) que no debe ser confundida con autenticación legal (fe pública y seguridad jurídica).

Por ello "se pretende en este trabajo esbozar la posibilidad de establecer un sistema de contratación electrónica con la participación de los notarios en la certificación y/o elaboración de los mismos, a fin de lograr un mayor grado de autenticidad, certeza y seguridad jurídica de dichos documentos, justamente por la aparición de un tercero ajeno a la relación contractual, con caracteres especiales de autenticación (dación de fe pública) quien con su intervención como testigo especial calificado, podría eventualmente tener la custodia de los documentos electrónicos que se efectúen en su presencia."[1]

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional ha puesto especial interés en que no se obstaculice la utilización de los modernos medios de comunicación, tales como el correo electrónico y el intercambio electrónico de datos (EDI), en la negociación de las operaciones comerciales internacionales y es por ello que recomienda una ley marco para que cada

[1] KEMPER (Ana María) Op.cit. p. 5

legislación nacional le dé validez y eficacia jurídica a los mensajes de datos sin soporte de papel.[1]

Ante este panorama en el uso de las modernas tecnologías, debemos analizar la necesidad de tutelar la seguridad y confianza de los contratantes en relación con las nuevas formas de contratación y comunicación. La participación de los Notarios en estos procesos comerciales llevados a cabo por medios electrónicos, ofrece una mayor aplicación de la fe pública que están investidos.

La participación de Notario en la elaboración de documentos electrónicos le daría certeza, seguridad y autenticidad a dichos documentos de manera similar a los documentos protocolares actuales.

Como sería esa participación? Que reglas se aplican? Se plantean nuevos problemas a resolver como el de la oferta y aceptación entre ausentes, el perfeccionamiento del acto jurídico, la manifestación del consentimiento, el lugar de emisión y recepción de la comunicación, etc.

Existen autores estudiosos del tema notarial que de manera muy conservadora sostienen que "solo podría intervenir el escribano en la elaboración

[1] Ley Modelo de la CNUDMI sobre Comercio Electrónico. Op.cit.p. 12

de documentación electrónica, en tanto y en cuanto estuviera en contacto directo con las partes, o por lo menos alguna de las partes contratantes. "[1]

Esta posición trata de conciliar el avance tecnológico con algunos principios clásicos de la función notarial, pero como veremos posteriormente la presencia del Notario será virtual, ampliando su campo de acción.

Para la validez de esta nueva labor notarial es preciso adecuar conceptos tan tradicionales como el de **"la unidad del acto"**, ya que por razón de la realidad actual este concepto tiende cada vez más a desaparecer en su concepción clásica.

Desaparece la concepción de la unidad del acto, como unidad temporal y espacial propia de la expresión del consentimiento contractual; tanto material, cuando se exteriorizan las voluntades ante la presencia del Notario, como formal, cuando el contenido de las voluntades queda plasmada en un solo instrumento.

Con la contratación electrónica se varía este concepto, ya que lo único que se mantiene inalterable es la parte formal, o sea las expresiones del consentimiento en un solo documento, dando lugar a lo que podría denominarse **"unidad de texto".**[2]

La actividad del cibernotario en el sistema latino, sería una función complementaria a la que realiza hoy día, ya que además de realizar la función

---

[1] KEMPER (Ana Maria). Op.cit.p. 7
[2] GAETE GONZALEZ (Eugenio) La Firma Electrónica y la Firma Digital. Op.cit. p. 19

propia en que se requiera la intervención notarial, podría certificar las firmas digitales de documentos electrónicos privados.

Para que nuestro sistema notarial utilice todos los avances tecnológicos que en cuanto a comunicación, la informática y la Internet nos ofrecen, no solamente es necesario que se aprueben leyes que autoricen el uso de los mensajes de datos, de la firma digital y los certificados digitales, sino que se requiere crear una cultura y estudio sobre la implicación y uso de dicha tecnología. Es necesario que los Notarios entiendan de sistemas operativos, del manejo del computador, de cuándo, porqué y cómo se debe guardar la información, y sobre todo de comprender que debe actualizarse conforme evoluciona internet y la tecnología que esté a disposición.

¿Qué conveniencia existe con la intervención notarial en la documentación electrónica?

En la contratación tradicional, el Notario ejerce un control de legalidad sobre el contenido jurídico del negocio, comprobando que el negocio cumple con los requisitos que el ordenamiento jurídico exige para su validez.

Este es uno de los varios aspectos por los que convendría la intervención del notario, ya que por un lado su intervención conllevaría un reconocimiento o control legal sobre la transacción y por otro lado, habría un control sobre la

seguridad tecnológica de dicha transacción que quedaría asentada y archivada en matrices electrónicas bajo su custodia, la cual podría consultarse siempre, con la seguridad de que no podría ser alterada por las partes el contenido del contrato una vez finiquitado y archivado en la matriz electrónica.[1]

Esa conveniencia se da por que el Notario como funcionario investido de la Fe Pública que le ha delegado el Estado para el ejercicio de su función, es el único autorizado para elaborar y/o certificar instrumentos electrónicos, y/o certificar firmas digitales en aquellos documentos electrónicos privados.

Debemos estar seguros de que es posible concebir un sistema que, sin menguar las labores de asesoramiento y control de legalidad que actualmente desarrolla el Notario, pueda obtenerse los beneficios propios de la agilidad que la contratación electrónica lleva consigo, dotándola de fe pública.[2]

El rol del Notario Público es primordial en el sustento de la legalidad de los procesos de certificación digital, pues con una herramienta diferente tiene la posibilidad de trasladar al mundo virtual el valor de la fe pública que se ejerce en el mundo real.

---

[1] LEAL NERY (Hugo) El Protocolo Cibernético Revista Electrónica de Derecho Informatico.N° 33 Abril, 2001. **www. acertia.com,** documento sin numeración de paginas

[2] RUIZ-GALLARDON (Miguel) Fe Pública y Contratación telemática. Derecho de Internet. Contratación Electrónica y Firma Digital. Op. Cit. P. 115

Aunque la participación de los Notarios en los procesos comerciales realizados por medios electrónicos va evolucionando de forma paulatina, también es cierto que los derechos y obligaciones de los contratantes "electrónicos" seguirán siendo exigibles como en la vía tradicional y es ahí donde la función del Notario es determinante para otorgar certeza y legalidad a las partes. [1]

En países como México, que ya han desarrollo el tema de la función notarial en cuanto a las Autoridades de Certificación, se ha sostenido que los Notarios Públicos "prestarán diversos servicios de certificación digital sustentados en la fe pública ejercida sobre la certificación de la identidad de personas y su reconocimiento expreso sobre el uso de un certificado para firmar digitalmente, o sobre el reconocimiento de la titularidad de un sitio web y las consecuencias legales de operarlo.[2]

Hemos analizado que para dar la seguridad que fundamente la certeza y la eficacia jurídica de los documentos electrónicos, se recurre al uso de la firma digital avanzada con método de encriptación asimétrico, que garantiza que los mensajes sólo podrán ser vistos por el destinatario de los mismos y con ello asegurar la integridad, autenticidad, confidencialidad y el no repudio del mensaje.

---

[1] **www. acertia.com** El Rol del Federatario en la Economía Digital, documento sin autor y sin numeración de página.
[2] Ibid.

Para que dicha firma digital tenga esa eficacia, debe estar sustentada en la intervención de terceras partes de confianza, que mediante los servicios de certificación, garantizarán la asociación de la clave con una persona determinada y que la identifique como el titular de la clave.[1]

Es en este momento en que la figura del Notario Público es necesaria, porque cuando se requiera un documento con autenticación legal, será su firma digital la que garantizará frente a terceros la integridad y el origen del mensaje.

Como podemos notar no solo mediante la firma digital avanzada se soluciona el problema de la identificación de las partes en los actos jurídicos realizados a través de internet, sino que la figura del Notario Público deberá estar presente cuando la autoridad de Certificación certifique a las partes, pues se cerciorará de la identificación del titular del certificado. Se traslada la identificación tradicional de los documentos oficiales de identificación, como la cédula de identidad y el pasaporte, a los medios electrónicos de identificación.

Por ejemplo la legislación comercial mexicana, contempla que, cuando los actos jurídicos requieran de la fe pública de un Notario (también se da la figura de los Fedatarios Públicos), como forma de darle certeza y seguridad, el acto deberá

---

[1] CORNEJO LOPEZ (Valentino). Una realidad Mexicana, la Firma Electrónica y la Participación del Notario Mexicano. Revista Electrónica de Derecho Arbor, Agosto, 2000. **www.derecho.org.v/lex.com,** documento sin numeración.

constar en un instrumento público conforme a la actividad del notario publico, donde emergen dos nuevos conceptos netamente cibernéticos: el notario cibernético y el protocolo electrónico.[1]

El proyecto de ley costarricense recoge una norma similar al establecer que *"Cuando una ley requiere que un documento o firma esté certificado o autenticado notarialmente por un abogado o de cualquier otra forma reconocido, verificado o certificado. tal requisito se tendrá por cumplido si una firma electrónica avanzada de un notario público, abogado, funcionario público o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma digital o firma digital avanzada."*[2] (El subrayado no es del original.)

Cuando se habla de una tercer parte de confianza que otorgue seguridad en la contratación electrónica, se requiere la figura de las Autoridades de Certificación y del cuando legalmente se requiera.

Para que el Notario ejerza esa labor de autenticar o certificar documentos firmados electrónicamente que contengan actos o contratos, será necesario que

---

[1] CORNEJO LOPEZ (Valentino). Una realidad Mexicana, la Firma Electrónica y la Participación del Notario Mexicano. Op.cit. Otro ejemplo es Colombia, que mediante Ley 588-2000, Reglamentó el ejercicio de la actividad notarial electrónica.

[2] Proyecto de Ley sobre Firma Digital y Certificados Digitales. artículo 6.

exista una Autoridad de Certificación Digital del Notario Público que lo acredite para prestar este servicio, surgiendo el concepto de Notario Cibernético[1].

Este será un Notario en que las partes confían y acuerden que presencie el acto jurídico por el medio electrónico en que se va a celebrar. La presencia del Notario será virtual a través de un computador que tendrá los requisitos de seguridad y confiabilidad exigibles para que pueda dar fe pública de dicho acto. [2]

Como funcionaría la participación del Notario en un contrato electrónico? Veamos un ejemplo hipotético:

Dos empresas que se contactan a través de una página de internet, deciden realizar un contrato electrónico y recurren con un tercero que actúa como testigo electrónico para darle seguridad y certeza jurídica. Para ello se asiste electrónicamente a un Notario Público facultado para otorgar fe de este tipo de acto de comercio y se establece un contacto virtual entre las tres partes: se presenta la oferta y la aceptación de los contratantes, la cuales pasan por el computador del Notario, este identifica a las partes por sus firmas electrónicas, la vigencia de las mismas, la de sus certificados digitales, la verificación de su representación y realizado todo ello certifica el acto con su propia firma digital, otorgando fe

---

[1] CORNEJO LOPEZ (Valentino). Una realidad Mexicana, la Firma Electrónica y la Participación del Notario Mexicano. Op.cit.

[2] CORNEJO LOPEZ (Valentino) Testigos Electrónicos ante la Dificultad de la Contratación Electrónica en el Derecho Mexicano. Revista Electrónica de Derecho Arbor, 2000. **www.derecho.org.v/lex.com,** documento sin numeración

pública al mismo. El Notario estará obligado de guardar en su forma original el contrato para su consulta posterior en caso de que exista un conflicto entre las partes.

Otro ejemplo sería que una parte se presenta ante el Notario y en su presencia realiza el acto y contrato, procediendo el mismo a darle autenticidad legal al instrumento con su firma digital.

En ambos casos el Notario Público debe estar capacitado para otorgar ese servicio y se debe conjuntar la labor de la Autoridad Certificadora con la del Notario para otorgarle así a la certificación la fe pública que por su naturaleza es inherente a la función notarial.

Como expusimos supra en cuanto a los conceptos y clasificación de fe pública, una parte de la función notarial es la fase autenticadora en la que el Notario imparte fe pública a los hechos o actos jurídicos ocurridos en su presencia,[1] por lo que debemos concluir que se debe integrar dentro de dicho concepto, la fe pública informática como una nueva actividad del Notario en que autentica actos realizados en forma virtual.

El Estado dentro de su poder de imperio y con el fin de brindar seguridad jurídica a la sociedad, debe otorgar al Notario Público la facultad de dar fe pública

[1] Ver supra, Título I, Capítulo I, Sección II, Fe Pública Notarial

no solo en aquellos actos realizados en forma documental, sino en todos en que la ley lo establezca como requisito, donde podremos incluir a los documentos electrónicos. [1]

Es en el momento en que intervenga el Notario dando fe pública de los actos realizados electrónicamente, satisfaciendo los requerimientos jurídicos propios de la teoría de la contratación, del acto formal de la escritura y de la labor notarial, que los documentos informáticos puedan llegar a constituir instrumentos públicos notariales.

La actuación del Notario permitirá dotar al documento de autenticidad en los siguientes aspectos:

1- En cuanto a la identidad de la parte ene l contrato que solicite su intervención,

2- En relación con su capacidad para actuar,

3- En lo relativo a la exactitud de su contenido y la fecha. No precisamente en cuanto a la verdad de las declaraciones, sino en lo que relativo a que es ése y no otro el contenido del documento que fue enviado, lo que se corrobora con la aplicación de un hash.

4- En cuanto a la verificación de la firma,

---

[1] CORNEJO LOPEZ (Valentino) Una realidad mexicana, la Firma Electrónica y la Participación del Notario Mexicano, Op. Cit., documento sin numeración de página.

5- En lo relativo a las garantías otorgadas en la celebración del contrato,

6- En lo que se refiere al secreto y la conservación del contrato, debe cumplir con la función de conservación y archivo del documento.[1]

En cuanto a la seguridad siempre salta la pregunta, sobre la posible intromisión de terceros ajenos (hackers) al documento electrónico en el momento de efectuarse la transmisión. Esta intromisión es posible, al igual que es posible falsificar y alterar documentos escritos en papel o documentos de identidad.

Si un hacker logra acceder un documento en el momento de efectuarse una transmisión o en su archivo, logrando pasar la dificultad de desencriptar una clave asimétrica, estaríamos ante un caso concreto de un delito idéntico al hecho de falsificación y alteración de un documento escrito en papel.

Entendido de que el Notario podrá ejercer una función importante otorgando fe pública a los actos y contratos realizados electrónicamente, debemos dejar claro que no todo Notario Público podrá realizar la función de Cibernotario.

---

[1] GAETE GONZALEZ (Eugenio) Firma Electrónica y Firma Digital. Op. Cit. P. 15 En la práctica la actuación notarial informática se limita al otorgamiento del certificado en la cual constan los datos apuntados, además de la identificación del Notario y del acompañamiento de la llave pública del cliente, debidamente cifrada, para su desencriptamiento por el destinatario o contraparte del contrato.

Para que un Notario pueda autenticar cibernéticamente será necesario:

1- ser un Notario Público debidamente habilitado en el ejercicio de la profesión;

2- Tomar un curso de certificación digital, el cual debe ser impartido por una "Autoridad" técnica en la materia (pública o privada) y debidamente autorizada por el Estado;

3- Obtener la licencia o permiso de la Dirección Nacional de Notariado, para realizar esa labor especial dentro de la función notarial; y

4- Debe adquirir el equipo (software) necesario para el proceso de certificación.[1]

La licencia o permiso para ejercer la función notarial cibernética no podrá ser indefinida, sino que deberá tener vigencia por un tiempo determinado. Esto en razón que dichos Notarios deben actualizarse en los temas informáticos atinentes a la seguridad de la certificación digital, por la evolución de la tecnología aplicada en la internet.

Es válido estimar que desde el momento en que las funciones notariales puedan ser realizadas electrónicamente, será aplicable a todas las demás materias

[1] Estos requisitos que, consideramos son plenamente válidos para nuestro país, son los que se solicitan en los Estados Unidos Mexicanos y están en su sitio web: **www.notariadomexicano.org.mx.** Asimismo son las condiciones generales exigidas en otros países como en los Estados Unidos de América.

(comercial, civil, penal, etc.), que puedan ejecutarse técnicamente por la vía computacional, al igual que lo hace en la actualidad con lo propio de su función.

La labor de Notario Cibernético ampliará la función notarial en los países con circunscripciones territoriales para el ejercicio del Notariado, como las impuestas por la ratio loci y que fueron expuestas cuando se desarrolló el tema de la actuación notarial extraterritorial.

El documento informático como expresión de la contratación a distancia es, por estructura y definición, un instrumento de carácter planetario, en el que las partes pueden estar en diferentes lugares y países, por lo que los Notarios deben tener en esta función una competencia universalista.

En cuanto a este punto el Dr. Eugenio Gaete, especialista en temas de derecho informático, sostiene que "apriorísticamente considerado el problema, nuestra posición es inclinarnos por otorgar a los notarios que actúen en materias de contratación a distancia una competencia *no limitada en cuanto al territorio*, la que quedará sujeta solamente al lugar de realización del contrato, entendiendo por tal, aquel en que se da fe de la última firma digital de éste, y ese notario proceda a imponerle su sello electrónico. [1]

[1] GAETE GONZALES (Eugenio) Firma Electrónica y Firma Digital. Op. Cit. P. 19

Asimismo y cuando avance el reconocimiento de firmas electrónicas otorgadas por autoridades de certificación de otros países, se podrá autenticar y certificar actos que se realicen con una de las partes que se encuentre fuera del país y cuyo acto tenga efecto en Costa Rica.

La Ley Modelo de la CNUDMI trata de que hayan relaciones económicas internacionales armoniosas, homologando las normas utilizables en el comercio internacional y electrónico en las diferentes legislaciones Se pretende que los actos y contratos realizados electrónicamente en un país, cumplan con los mismos requisitos del país donde tendrán eficacia legal.

El Proyecto de ley costarricense establece que los certificados de firma digital que sean emitidos por entidades del exterior, serán equivalentes a los otorgados por Certificadores nacionales, siempre y cuando sean homologados por alguno de ellos. Cuando un Entidad de Certificación homologue un certificado del exterior, lo hará bajo su responsabilidad, pero la Autoridad extranjera deberá ser reconocida por la Autoridad de acreditación competente y el certificado debe cumplir con los requisitos fijados por la ley, su reglamento y las normas internacionales.[1]

Esta actividad conllevará un ahorro económico y de tiempo, porque por un lado las partes no necesitarán asistir ante los Cónsules y pasar por las

[1] Proyecto de Ley de Firmas Digitales y Certificados Digitales. Op.cit. artículo 12.

legalizaciones requeridas para que los documentos otorgados fuera del país puedan tener efectos en Costa Rica y por otro, los Notarios nacionales no tendrán que desplazarse fuera del país para autorizar actos y contratos para ser efectivos en nuestro país.

"No obstante cada vez, se ve más la necesidad de crear las notarías electrónicas, como órganos públicos e imparciales de intermediación, en la comunicación de las partes contratantes, para poder, cuando se precise, elevar a una forma pública la contratación electrónica y dotarla de medios de prueba irrefutables tanto de su contenido como de las fechas de envío o recibo de los contratos o documentos. Determinando con ello la prueba de los derechos y obligaciones de las partes, el momento de su nacimiento y el de su extinción."[1]

[1] BARRIUSO RUIZ (Carlos) Op. Cit., p. 265.

CAPÍTULO SEGUNDO

PROTOCOLO DIGITAL

Si el tema del Notario Cibernético es polémico, el del "Protocolo electrónico" es mucho más complicado, porque siempre habrá opositores a la posibilidad de implementar en formato digital uno de los iconos de la actividad notarial de sistema latino, la de ser eminentemente escrito.

Ante la posibilidad del "Protocolo Electrónico" surge la interrogante de cuales serán los medios que el Notario utilizaría para resguardar esa versión íntegra de los mensajes?

Se deben considerar siempre los medios o el medio más seguro, pues están los medios magnéticos como el diskettes, cartuchos Zip o Jaz y los medios ópticos de almacenamiento de datos como los CDS, en los que pueden constar los mensajes de datos intercambiados entre el Notario y las partes o intervinientes, así como las respectivas firmas o certificados digitales que aseguren que dichos mensajes provienen de quien deben provenir.[1] Estos medios serán las referencias o apéndice, en la que se coleccionan los documentos y demás elementos materiales relacionados a que se refieren los instrumentos que formarán parte integrante del "Protocolo digital".

En cuanto a este sistema de archivo de documentos públicos electrónicos, o llámese protocolo electrónico o soporte virtual, siempre vendrá a colación el tema

[1] LEAL NERY (Hugo) Op.cit.

de la seguridad. Con mucha razón los detractores de la inserción de la electrónica en el notariado siempre argumentarán, que dicho protocolo es menos seguro que el protocolo tradicional, pues en la electrónica pueden surgir eventualidades donde se pierdan datos o no se puedan acceder a ellos, o hayan acceso no autorizados (hackers o crackers), etc.

Es por esto que se debe idear un sistema de respaldos de la información, ante la eventualidad de pérdida de información o su actualización, que deberá estar bajo custodia del Notario y de alguna Autoridad, como lo es en nuestro país el Archivo Nacional, que puedan sustituir la información perdida o colapsada o volver a archivar la información en un sistema más seguro conforme el avance de la tecnología.[1]

Aunque se dice que no hay sistema vulnerable, se deben establecer fuertes sistemas de seguridad como la encriptación y los "firewalls", para detener la intromisión de terceros no autorizados. Estos sistemas de seguridad deben también ser revisados periódicamente, ya que la tecnología está condenada a rebasarse a sí misma, por lo que los sistemas deben actualizarse.

Adoptando el sistema, estaremos ante ventajas como el ahorro de papel, la eficiencia en la labor notarial, la agilidad en la consulta, la agilidad en la búsqueda

[1] Hemos visto que la Procuraduría General de la República se manifestó que legalmente le corresponde al Archivo Nacional tomar las medidas que considere convenientes para el archivo de documentos.

de escrituras, reducción de tiempo y costos económicos en traslados de las partes o el Notario para otorgar y autorizar los documentos públicos, etc. Conforme caminemos por la tecnología, podremos experimentar todos los beneficios que su adaptación a la función notarial nos traería.

La idea de un "protocolo electrónico" no debe tomarse a la ligera y debe afrontarse con seriedad, por que estamos a las puertas de poder crear instrumentos públicos electrónicos[1], debemos ir pensando en el lugar donde se archivaran dichos instrumentos y el trato que le daremos a esos archivos.

Surgen muchas interrogantes en cuanto a los notarios cibernéticos y los protocolos electrónicos y muchos pensarán que nuestro país está muy lejos de que se den estos avances, porque nuestro sistema de notariado es netamente escrito y que los principios en que está sustentado como el de permanencia y el de unidad del acto no lo permitirían.

No debemos cerrarnos a los avances de la tecnología, más bien debemos analizar qué han hecho los otros países que han caminado dicha senda y pensemos cual va a ser el ámbito de aplicación de la documentación notarial electrónica en los actos y contratos inscribibles en el Registro Público. Este trabajo pretende ser

[1] El artículo 6 del Proyecto de Ley de Firma Digital y Certificados Digitales establece que cuando una ley requiera que un documento o firma esté certificado o autenticado notarialmente por un abogado, ese requisito se tiene por cumplido si la firma avanzada de un notario público es puesto o vinculada al documento o firma digital. A nuestro criterio este documento vinculado con la firma avanzada de un notario, sería un instrumento público electrónico.

una inquietud en cuanto al tema, que deberá desarrollarse ampliamente cuando se aprueba la legislación pertinente.

Para los que no creen en esta posibilidad y adelantándonos a los que desarrollaremos en las siguiente sección en cuanto a las experiencias que han tenido otros países, es interesante la resolución emitida por el Dirección General de los Registros y del Notariado en España, el 26 de Abril del año 2000, en la que estima que los requisitos de fondo como son las afirmaciones del Notario sobre la presencia, identificación y capacidad de las partes otorgantes, lectura del documento y consentimiento de éste a su contenido, advertencias legales, etc., que en cada caso sean requeridos, no se verán afectados por el uso de transmisión telemática utilizando la firma electrónica. En cuanto a los requisitos de forma, como por ejemplo el sello y numeración de folios, dicha resolución estima que los mismos deben ser interpretados de acuerdo a su finalidad y que si se garantiza la autenticidad del documento, no cabe que tales formalidades sean obstáculo para el empleo de la firma digital en el ámbito notarial. [1]

Aquí surge la interrogante de que si estamos preparados para la inserción de un "protocolo digital"?

---

[1] MAESTRE (Javier A.) El empleo de la Firma Electrónica en el Sistema Registral Español.: Comentario a la Resolución de la Dirección General de los Registros y del Notariado, de 26 de abril de 2000. Revista Electrónica de Derecho Informático. www.publicacionesderecho.org/redi. Documento sin numeración de página.

Los especialistas en informática establecen que tecnológicamente contamos con los medios y el personal técnico para implementar esos archivos y sobre todo para enseñar a los Notarios las técnicas de archivo digital.

Por otro lado, sostienen que conforme a la definición y las características contempladas en el articulo 43 del Código Notarial para el Protocolo, es perfectamente viable considerarlo no solamente de papel, pues la norma no lo establece así. Para ello exponen que el protocolo podría ser un libro digital que tendría las siguientes características:

- Plenamente identificable con un número de serie.
- Con un número de folios preciso y numerados.
- Con un formato de página inmodificable.
- Con mecanismos de integridad.
- Con estampado cronológico y posterior firma digital.[1]

Indudablemente nos falta camino por recorrer, pero en Costa Rica el Centro Nacional de Tecnología está llevando a cabo junto con la empresa privada, una toma de conciencia del nivel tecnológico que tiene el país y de los usos que se le puede dar a dicha tecnología. El Ministerio de Ciencia y Tecnología también está realizando grandes esfuerzos para que el país se inserte en el avance tecnológico.

---

[1] AGUILAR SANCEHZ (Edwin) Notariado Digital en Costa Rica. Op. Cit. p. 5

En cuanto a la figura del Notario Cibernético y el Protocolo Electrónico, el Instituto Centroamericano de Administración Pública ICAP, está coordinando con la Dirección Nacional de Notariado, El Registro Público, El Instituto Costarricense de Derecho Notarial, para que se vaya aceptando su necesidad, su figura y sobre todo su realidad.

Entendemos que deberá existir una normativa notarial que establezca la regulación de los notarios cibernéticos, admitiendo dicha figura y puntualizando los requisitos para obtener dicha licencia.

Como podemos observar el tema se está discutiendo, prueba que la sociedad está frente a dicha realidad tecnológica, la cual debe tener repercusión en las relaciones sociales y comerciales, las que deben ser reguladas por el Derecho.

No cabe duda que los Notarios no pueden estar ajenos al fenómeno de la digitalización, ni antagónicos a ese fenómeno, sino que deberíamos aprovechar la ocasión para dar entrada a la fe pública notarial en el mundo del Comercio Electrónico.

Debemos avanzar primero en el plano teórico tanto informático como jurídico de las transacciones inmobiliarias electrónicas, para ir en la práctica paso a paso, conforme la experiencia lo permita.

SECCIÓN II: EXPERIENCIAS EN PAISES DE NUESTRO SISTEMA

Esta discusión ya se ha librado en otros países, por lo que es interesante hacer un resumen de lo que se ha dicho al respecto de los archivos digitales.

Así vemos que cuando en México se discutió la factibilidad de que en un futuro se estableciera un soporte electrónico del Protocolo Notarial, la Lic. Ivonne Muñoz Torres, Coordinadora del Comité de Publicaciones de la Academia Mexicana de Derecho Informático manifestó: "Desde el punto de vista, en el caso de los países donde existe el Notario de tipo latino, el soporte electrónico del protocolo jamás podrá desplazar por completo a el protocolo que existe en soporte papel, no es que me niegue a que se deben de explotar las bondades de la informática, menciono lo anterior porque si hay algo que le da certeza jurídica al cliente del Notario, es el soporte papel. Además, debes recordar que para el caso del notariado latino clásico, dentro de sus principios notariales, tenemos aquel conocido "Principio de Permanencia" en donde se habla de que aún cuando el notario ya no exista (por cualquier razón, la cual generalmente es la muerte), el documento físico sigue existiendo tanto depositado en el archivo de la notaria (dentro de los plazos indicados en función de lo que indique cada legislación) como en el Archivo General de Notarías y/o Registro Público de Comercio o de la

Notarias y Registros transferir sus protocolos en formato digital, pero un año después no se conocía de ninguna que lo hubiere hecho.[1]

En Perú el reconocimiento del documento digital y su archivo se da a raíz del problema de la falta de espacios en los archivos físicos y la dificultad para la obtención de la información de documentos escritos, llevó a que mediante el Decreto Legislativo de "Normas que regulan el uso de tecnologías avanzadas en materia de archivo de documento e información" se reconociera valor jurídico y probatorio a la documentación producida a través de la microfilmación y a sus reproducciones como copia autenticada o mediante micro duplicado.

Para tener valor jurídico, el procedimiento de digitalización de un documento debía cumplimiento con normas técnicas internacionales, que garantizaran la fidelidad o integridad de la reproducción, la durabilidad e inalterabilidad similar al documento original y la capacidad de reproducirlo a un medio convencional (documento escrito). Este procedimiento debía efectuarse bajo lo dirección y responsabilidad de los depositarios de la fe pública (Notarios), quienes además estaban en la posibilidad de autenticar los documentos obtenidos en dichos

[1] Mensaje de correo electrónico dirigido por José Ovidio Salgueiro, especialista venezolano en Derecho Informático, a Hugo Leal Neri el 02 de Abril del 2000, citado por LEAL NERI (Hugo) Op. cit

archivos que tendrían el mismo valor que los efectuados por medios convencionales.[1]

El Profesor Chileno, Eugenio Gaete, sostiene en cuanto al tema de los sistemas de archivo y reproducción de los instrumentos públicos que " se hace necesario estudiar los sistemas de archivo de protocolos, comparándose con los modernos sistemas electrónicos, caracterizados por la seguridad que brindan, por la responsabilidad a que quedan sujetos los denominados terceros proveedores de servicios que son quienes los tienen a su cargo, por los medios técnicos con que cuentan, tanto respecto de su conservación como de la reproducción mediante copias, aún cuando es preciso tener en consideración que de lege ferenda, deberá ser el Notario el último responsable de su custodia, guarda, conservación y reproducción."[2]

Concluye el Profesor Gaete que el sistema de archivo de los instrumentos públicos electrónicos, que no sería otra cosa que un "protocolo electrónico", debe consistir en un soporte seguro, durable e inalterable que tenga la información encriptada, con recuperación direccionable de datos, como por ejemplo el sistema de thesaurus, cuya conservación y certificación estén a cargo del Notario Público

[1] SEGURA LOARTE (Alejandro) Hacia el establecimiento del documento digital en el Perú. Revista electrónica de Derecho Informatico. www.publicacionesdereco.org/redi, documento sin numeración.
[2] GAETE GONZALEZ (Eugenio Alberto) Documento Electrónico e Instrumento Público. Revista Electrónica de Derecho Informático. N° 24. Julio. 2000, en **www.derecho.org.v/lex.com**, documento sin numeración de pagina.

como autoridad certificadora y que esté provisto a través del proveedor de servicios para que puedan emitir copias electrónicas de los documentos que contiene.[1]

También resulta interesante la puesta en marcha por el Registrador de la Propiedad de Guatemala, el Lic. Rolando Barrios, de la modernización de los Registros de la propiedad en ese país, y básicamente de Ciudad de Guatemala, los cuales a partir de 1999 se encuentran totalmente informatizados. En lo relativo a su guarda y conservación, ésta se realiza en micro filmaciones, de las cuales, por ley, existen tres ejemplares originales: el primero guardado en el Registro, el segundo en las Bóvedas del Banco de la Nación, y el tercero (he aquí una novedad) en el Archivo de Indias de Sevilla, por especial convenio con el Ministerio de Justicia de España.[2]

Pareciera que el buen criterio impondrá que se vaya avanzando lenta, pero seguramente en el establecimiento de la escritura electrónica y el protocolo electrónico.

Un ejemplo al respecto, puede ser el del Conservador (Registrador) de Bienes Raíces de Santiago de Chile, el cual, por ley debe mantener sus protocolos en

---

[1] Ibid

[2] Mensaje de correo electrónico dirigido por el Dr. Eugenio Gaete a Hugo Leal Neri, el 29 de Diciembre del 2001.

papel, pero voluntariamente, lleva un sistema paralelo de archivos microfilmados, destinados a permitir la consulta rápida, limpia y eficiente de las inscripciones. Con ello se impide el manoseo y deterioro de los libros, y se gana en tiempo a través de la búsqueda electrónica de las inscripciones.[1]

En Buenos Aires, Argentina, el sistema de inscripciones lleva archivándose en forma informatizada, desde fines de la década de los sesenta y no ha habido fallas en él.

Si bien las posibilidades técnicas están dadas, lo cierto, es que se trata de una materia en la cual es preciso caminar con sumo cuidado, por los aspectos de fe pública involucrados, y sobre la cual descansa todo el sistema de bienes inmuebles.

Como podemos ver, no es cuestión únicamente de impulsar un cambio, sin medir las posibles fallas que se pueden dar en la seguridad y tratar de solucionarlas antes de tiempo.

[1] Mensaje de correo electrónico dirigido por el Dr. Eugenio Gaete a Kadir Cortés Pérez el 29 de Diciembre del 2001.

CAPÍTULO TERCERO

NUESTRA REALIDAD NACIONAL

SECCIÓN I: NOTIFICACIONES POR MEDIOS ELECTRÓNICOS.

En el desarrollo de los temas sobre la firma, los certificados digitales, las Autoridades Certificados y el Notario Cibernético, hemos procurado analizar algunas normas que contiene el Proyecto de Ley de Firmas Digitales y Certificados Digitales.

En este último capítulo se determinará, qué normas existen en nuestro ordenamiento vigente que permitan el uso de los documentos electrónicos como documentos con plena validez y eficacia legal, así como las instituciones que podrían dar algunos de los servicios para la implementación del notariado cibernético, iniciando con las notificaciones por medios electrónicos.

Para el Profesor Guillermo Augusto Pérez Merayo no existen en Costa Rica reglas que habiliten aspectos básicos para el comercio electrónico y el reconocimiento de los mensajes de datos. Considera el Lic. Pérez Merayo que la Ley de Notificaciones, Citaciones y otras comunicaciones judiciales, es la única ley que permite el uso de un medio electrónico (fax) para realizar notificaciones.[1]

Esta afirmación del Lic. Pérez Merayo no es totalmente exacta, ya que el artículo 6 de la Ley a la que hace referencia establece además del fax, "*cualquier otra*

[1] Charla realizada en el Centro Nacional de Alta Tecnología sobre Nuevas Tecnologías de Comercio Electrónico, el 15 de Mayo de 1999, en que participó el Lic. Guillermo Augusto Pérez Merayo

forma que permita la seguridad del acto de comunicación" y seguidamente dice que dichos documentos *"tendrán la validez y eficacia de un documento original siempre y cuando quede garantizada su autenticidad, integridad y el debido cumplimiento de las leyes procesales"*. Parece que el legislador estaba preparando el camino para la notificación por medios electrónicos más allá del fax.

Esta apreciación tiene su confirmación con la promulgación por parte de la Corte Plena del Reglamento de Comunicaciones y Notificaciones por medios Electrónicos, que al efecto dispone:

> *"Se autoriza a los Tribunales de Justicia del Primer y Segundo Circuitos Judiciales de San José, para notificar resoluciones judiciales por medios electrónicos."* [1]

Así el Reglamento a la Ley de Notificaciones dispone todo lo relativo a la forma en que se realiza las notificaciones realizadas por medios electrónicos y la eficacia que se le otorga a esta notificación. Lo único que constará en el expediente será el acta de lo que fue realizado digitalmente.[2]

Esta normativa no es aislada, pues la Ley de Contratación Administrativa contempla la comunicación de actos de procedimiento de la

---

[1] Reglamento de Notificaciones y Comunicaciones por medios Electrónicos, # 15-2000, Artículo 1.
[2] Ibid, artículo 5.

Administración por medios electrónicos que garanticen la certeza de la recepción y el contenido del mensaje. el Reglamento General de dicha ley desarrolla la normativa de la comunicación de la Administración por medios electrónicos e incluso prevé la posibilidad de presentación de ofertas o aclaraciones por parte de los administrados.[1]

Este tipo de notificación también se ha ido previendo en otras normas reglamentarias sobre todo en la Administración, por cuanto es notorio el avance de la tecnología y el uso que puede dársele en la consecución de celeridad en los procesos.[2]

La utilización de las bondades de la tecnología información para integrar en un ambiente digital servicios y procesos de la Administración, crean lo que se ha denominado "El Gobierno Electrónico". Con ello se pretende una mayor eficiencia en la atención y respuesta de las instituciones gubernamentales para con el administrado y en las relaciones entre la propia

---

[1] Ley de Contratación Administrativa 7494 del 2 de Mayo de 1995, publicada en el Alcance 20 de la Gaceta 120 del 8 de Junio de 1995, Artículo 40 y Reglamento General de la Contratación Administrativa, #25038-H, artículo 43 en cuanto a comunicación por medios electrónicos, artículo 45 en cuanto a presentación de licitaciones públicas y artículo 100 en cuanto a la notificación en recursos de apelación, son algunas de las normas en que se contempla el uso de los medios electrónicos para el procedimiento de las contrataciones administrativas y sus recursos.

[2] Ejemplo de ello lo encontramos en el Reglamento de Procedimiento interno en trámite de quejas ante la Fiscalía del Colegio de Abogados de Costa Rica, Sesión # 12-99, que establece el correo electrónico como uno de los medios de notificación y en que momento se tiene por realizado el acto. También el artículo 48 del Reglamento de la Defensoría de los Habitantes, #22266-J, establece que la institución puede valerse de todos los medios electrónicos e informáticos disponibles para el levantamiento de expedientes.

administración, procurando más beneficios para el Estado pues se ahorra tiempo, dinero y se da una mejor y mayor recaudación de impuestos.

Dentro de ese enfoque del Gobierno Electrónico el Estado debe invertir en tecnología, realizar estrategias, crear políticas públicas que impulsen la utilización de la tecnología y crear leyes y reglamentos que lo permitan.

Es por ello que se dan leyes como las que hemos referido y como el Código de Normas y Procedimientos Tributarios, que a raíz de las reformas y adiciones realizadas en el año 1999, dispone la posibilidad de que los contribuyentes presenten sus declaraciones utilizando medios electrónicos, para lo cual se deben utilizar *"elementos de seguridad tales como la clave de acceso, la tarjeta inteligente y otros que la Administración le autorice al sujeto pasivo y equivaldrán a su firma autógrafa."* [1]

Hemos tratado comunicaciones por medios electrónicos, cuya constancia queda determinada en papel, pero esta última norma nos deja ver el uso de un documento debidamente firmado digitalmente.

---

[1] Código de Normas y Procedimientos Tributarios. # 4755, del 29 de Abril de 1971, publicado en el Alcance 567 de la Gaceta 117 del 4 de Junio de 1971, Título 4, Capítulo 2, Artículo 122.- Determinación por los contribuyentes y declaración jurada.

SECCIÓN II: RECONOCIMIENTO NORMATIVO DE AUTENTICACIÓN Y AUTORÍA DE LOS CARACTERES ELECTRÓNICOS.

Pero nos preguntamos, existe alguna norma vigente que reconozca validez y eficacia a una firma digital y a un documento electrónico?

Veamos primero la relativo a la firma digital.

En el año 1998 la Procuraduría General de la República señaló que el reconocimiento con valor jurídico de la combinación de caracteres electrónicos utilizados como firmas, no eran posibles, por cuanto la regulación de dichos medios de firmar documentos digitales debía ser creada por ley.[1]

Pero las reformas al Código de Normas y Procedimientos Tributarios del año 1999, incluyeron el reconocimiento de ciertos elementos electrónicos de seguridad para ser usados como firma de un documento de tal importancia como lo es una declaración jurada para la determinación de un impuesto.

---

[1] Procuraduría General de la República. Dictamen C-283-98, dirigida al Archivo Nacional el 24 de diciembre de 1998. Se incluye en el dictamen que las autoridades certificadoras deben ser creadas por ley,

Observemos que no estamos hablando de una firma digital avanzada como la estudiada, sino únicamente de ciertos elementos electrónicos de seguridad.

Esa misma línea de reconocimiento la encontramos en otra normativa relacionada con la Administración. La Ley General de Aduanas establece que:

> *"Los funcionarios, auxiliares de la función pública aduanera y demás usuarios serán responsables del uso del código de usuario y de la clave de acceso confidencial asignados y de los actos que se deriven de su utilización.*
>
> *La clave de acceso confidencial equivale a la firma autógrafa de los funcionarios, auxiliares y demás usuarios para todos los efectos legales."*[1]

Esta ley tiene en todo un capítulo dedicado a la "Aplicación de Sistemas Informáticos", en donde ratifica que el uso del código de usuario y la clave de acceso confidencial presume la titularidad del declarante y de los actos transmitidos electrónicamente, como una firma de dichos actos.

---

[1] Ley General de Aduanas. # 7557, del 20 de Octubre de 1995 publicado en la Gaceta 212 del 8 de Noviembre de 1995, Artículo 105.

Mediante el Reglamento a dicha ley se establece que el computador de la División de Estadística, Registro y Divulgación le asignará a las personas físicas y a los empleados y demás personal de personas jurídicas, la clave de acceso confidencial que deberá utilizarse para firmar documentos electrónicos, lo cual se realizará una vez al año.[1]

Como podemos ver claramente, estas leyes que incluyen la posibilidad de uso de códigos y claves de acceso confidenciales, incluyeron dichas normas en reformas de los años 1999 y 2000, poniéndose al corriente con las legislaciones de avanzada en el reconocimiento de los medios electrónicos de información.

En el campo de la Administración aduanera se ha camino mucho en cuanto a la validez de las transmisiones electrónicas y la firma de dichos mensajes, ya que el Código Aduanero Uniforme Centroamericano (CAUCAIII) establece los medios equivalentes a la firma autógrafa en su artículo 23, que reza:

"Las firmas electrónicas, los códigos, claves de acceso confidenciales o de seguridad equivalen, para todos los efectos legales, a

[1] Reglamento a la Ley General de Aduanas, Decreto 25270-H del 14 de Junio de 1996, reformado por Decreto 28976-H del 27 de Setiembre del 2000, Artículo 85

la firma autógrafa de los funcionarios y empleados aduaneros, auxiliares, declarantes y demás personas autorizadas." [1]

Existen muchos ejemplos más de normas, sobre todo reglamentarias, que permiten el uso de firmas electrónicas, por lo que es interesante lo que establece el artículo 414 del Código de Comercio.

Esta disposición legal establece que la firma reproducida por medios mecánicos no se considera eficaz, *"salvo los negocios, actos o contratos en que la ley o el uso lo admitan."*

Por lo anterior podemos concluir o colegir que siendo permitida por el uso y la costumbre, la firma digital será eficaz en los documentos, actos o contratos electrónicos que sean firmados de esa manera, los cuales servirán de plena prueba. El uso y la costumbre en la utilización de la tecnología es evidente, tomando en cuenta la posibilidad otorgada por diversas normativas y sobre todo en nuestros tiempos que es un uso común la realización de actos electrónicos que enviamos a través de internet.

Con lo anterior es evidente la necesidad de la aprobación de la ley de Firmas Digitales y Certificados Digitales para dar rango legal al principio de

---

[1] Código Aduanero Uniforme Centroamericano (CAUCA III) Nº 29046-COMEX, del 20 de Octubre del 2000, que pone en vigencia la Resolución 60-2000 del Consejo de Ministros de integración Económica COMIECO XV, Artículo 23.

equivalencia funcional a los objetos del ámbito atómico y del ámbito desmaterializado de las señales digitales. No podemos estar atomizando nuestra legislación de normas dispersas para poder utilizar medios diferentes a la firma ológrafa o haciendo interpretaciones para buscar la validez de dichos medios.

Si estamos usando algunos mecanismos de seguridad como códigos y claves para ser referidas como firmas electrónicas para autenticar documentos, se debe tener el sustento de los certificados digitales y de las Autoridades que permitan determinar la validez de esos mecanismos y que sean verdaderas firmas digitales.

Si no lo hacemos así, se estaría enviando un mensaje de incertidumbre sobre la tecnología a los usuarios y podríamos retroceder en nuestro intento de que el derecho se ajuste a la realidad social y al avance vertiginoso de la tecnología de la información.

La iniciativa en la aprobación de la Ley de Firmas Digitales, debe integrar todos los sectores de la sociedad civil, tanto público como privado. Como expresa el Master Christian Hess, "solamente de ese modo (vale decir, evitando legislar sobre la firma digital a partir de sus aplicaciones en sólo

algunas áreas concretas, como comercio, banca, etcétera) se puede garantizar que el resultado sea todo lo provechoso que puede ser para el país"[1]

Concluida la anterior afirmación, nos queda por ver qué sucede con los documentos electrónicos.

SECCIÓN III: NORMATIVA ACTUAL QUE RECONOCE EL DOCUMENTO ELECTRÓNICO

Al igual que con la firma realizada por medios electrónicos, encontramos algunos normas dispersas en nuestra legislación que le dan validez y eficacia a los documentos electrónicos en ciertos sectores.

Así encontramos que las notificaciones de resoluciones judiciales, de resoluciones, comunicaciones y de actos de la Administración realizadas por medios electrónicos, no es más que el reconocimiento de la validez de dichos documentos electrónicos y de la eficacia de dichos mensajes.

Recordemos, como ejemplo lo que dice la Ley de Notificaciones en cuanto a los documentos notificados por medios electrónicos: "*tendrán la*

---

[1] HESS ARAYA (Christian) Comentarios al proyecto de Ley de Firma Digital de Costa Rica, enviado al Dr. Luis Paulino Mora, Presidente de la Cortes Suprema de Justicia, el 19 de Febrero del 2001, www.comunidad.derecho.org/chess.

validez y eficacia de un documento original siempre y cuando quede garantizada su autenticidad, integridad y el debido cumplimiento de las leyes procesales [1]

También encontramos en la Ley General de Aduanas tiene varias normas que reconocen los datos y registros electrónicos como prueba de los mismos y expresamente establece que el documento que prueba la existencia del contrato de transporte multimodal puede ser obtenido por medio de transmisión electrónica de datos, el cual se considera un documento de circulación al portador, a la orden y no negociable.[2] Estos datos, registros y contratos de transporte no son más que documentos electrónicos reconocidos por ley.

Una norma muy interesante es la contenida en la Ley Reguladora del Mercado de Valores, que permite el traspaso de valores representado por medio de anotaciones electrónicas, el cual es oponible a terceros desde que se practica la inscripción contable de la anotación electrónica. [3] La Ley está permitiendo el trasiego de valores por medios electrónicos, sin necesidad del

---

[1] Ley de Notificaciones, Citaciones y otras comunicaciones judiciales, artículo 6
[2] Ley General de Aduanas, Artículo 148.
[3] Ley Reguladora del Mercado de Valores, #7732 del 17 de Diciembre de 1997, publicado en la Gaceta # del 27 de Enero de 1998.

papel, reconocimiento plena validez a la anotación electrónica del traspaso.[1]

Esta Ley además reformó algunas normas del Código de Comercio, para el reconocimiento de los medios electrónicos dentro de la actividad bancaria. Nos interesa reproducir lo establecido en nuestra ley comercial para la certificación del detalle de los cheques pagados por los bancos, ya que dispone que lo harán mediante *microfilmación, imagen digital o archivo electrónico... La microfilmación o la imagen digital certificada constituirán plena prueba con respecto a todos los documentos relaciones con la operación de las cuentas corriente y tendrán el mismo valor legal que el documento original.*"[2]

Existen más ejemplos de cómo se reconocen los documentos electrónicos, como sería la comunicación que realizan los Juzgados de Tránsito al Registro de la Propiedad de Vehículos Automotores, de los gravámenes de los vehículos para que estos sean anotados sobre los vehículos.[3]

---

[1] En cuanto al tema del trasiego de valores considero que sería aplicable en Costa Rica la Propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales, donde se pide a los operadores financieros comprobar la identidad de sus clientes y tener toda su información.

[2] Código de Comercio, y sus reformas. Ley 3284, 1964. Sistemas Legales Master Lex, artículo 632.

[3] Ley General de Tránsito por vías públicas terrestres, #7331 del 13 de Abril de 1993, reformada con la vigencia del Código Notarial en el año 1998.

La Ley Orgánica del Poder Judicial tiene una disposición muy interesante, tanto en lo referente al reconocimiento de los documentos digitales, así como a los archivos electrónicos.

Al respecto el artículo 6 bis de la citada ley dispone:

" *Tendrán la validez y eficacia de un documento físico original, los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos o producidos por nuevas tecnologías, destinados a la tramitación judicial, ya sea que contengan actos o resoluciones judiciales. Lo anterior siempre que cumplan con los procedimientos establecidos para garantizar su autenticidad, integridad y seguridad.*"[1] (Lo resaltado no es del original)

Como podemos ver, la Ley Orgánica del Poder Judicial establece en esta norma los parámetros doctrinarios que hemos desarrollado en esta investigación y las corrientes legislativas internacionales para el reconocimiento de los documentos electrónicos en todas sus modalidades y sus correspondientes archivos.

---

[1] Ley Orgánica del Poder Judicial, # 7333, Capítulo Uno, Artículo 6 bis, párrafo primero. Edición Electrónica de Sistemas Legales Master Lex. 1993.

Esta disposición fue adicionada a la Ley Orgánica del Poder Judicial, mediante la Ley de Reorganización Judicial # 7728 del 15 de Diciembre de 1997, publicado en el Alcance #61 de la Gaceta #249 del 26 de Diciembre de 1997, y contiene una visión muy actualizada por cuanto no solo hace el reconocimiento de los mensajes de datos electrónicos, sino que sugiere el reconocimiento de otros documentos o soportes que sean producidos por el avance de nuevas tecnologías.

Reconoce plena validez y eficacia a los documentos o archivos digitales, siempre que cumplan con los procedimientos que garanticen la autenticidad, integridad y seguridad de los mismos.

Cuando un Juez consigne actos o resoluciones en medios electrónicos, la norma establece que no será necesaria su impresión ni su firma, si los medios de protección del sistema hacen que se pueda acreditar su autenticidad. Está autenticidad como hemos explicado, se logra con la seguridad y la integridad del sistema de firma digital empleado.

Esta norma se complementa con lo dispuesto en el Artículo 368 del Código Procesal Civil, en cuanto establece una definición amplísima de documento pues reconoce como tales "*en general, todo objeto mueble que tenga carácter de representativo o declarativo.*" pretendiendo no amarrar los medios

de pruebas al avance de la tecnología y a su incorporación como medios de prueba en juicio.

Esta disposición al igual que las contenidas en la Ley de Registro, Secuestro y examen de documentos privados e intervención de las comunicaciones[1], evidencian el intento del legislador de que nuestro derecho positivo de incorporar dentro del elenco documental, todos los medios producidos por el cambio tecnológico.

La Procuraduría General de la República en consulta del Archivo Nacional reconoce la existencia de "una serie de normas en el ordenamiento jurídico para la producción y gestión de documentos, así como de los producidos por medios automáticos, léase **documentos electrónicos**."[2]

Este Ente concluye que luego de analizar el documento electrónico, su función, su contenido, los criterios de seguridad y sus requisitos fundamentales, un disco compacto constituye un documento con valor jurídico de conformidad con nuestro ordenamiento, en tanto y cuanto se

---

[1] Ley de Registro, Secuestro y examen de documentos privados e intervención de las comunicaciones, #7425 del 09 de Agosto de 1994, que en su artículo primero autoriza el registro de cualquier documento privado que sea indispensable para esclarecer asuntos penales, dentro de los cuales se incluyen cualquier medio de carácter representativo o declarativo, como el electrónico.
[2] Procuraduría General de la República. Dictamen C-283-98.

pueda emitir, archivar y reproducir los documentos electrónicos contenidos en el.[1]

Es interesante analizar que los documentos electrónicos no son "algo extraño" a nuestra realidad social, pues conocemos su existencia y de su utilización, pero somos tímidos a la hora de darle validez y eficacia a los actos que en el se contenga.

Las disposiciones citadas nos indican que para efectos judiciales tienen eficacia, validez y fuerza legal tanto los documentos atómicos (por ejemplo en papel), como los documentos electrónicos.

Con base en lo anterior cualquier persona podría usar como prueba un documento electrónico, así como usa un documento de papel, siempre que la información contenida sea accesible y pueda ser usada como referencia posterior.[2]

En cuanto a este tipo de documentos, con la legislación vigente y aún con la aprobación del proyecto de Ley sobre Firmas Digitales y Certificados Digitales, para ser utilizado como prueba, se tendrá que aplicar las reglas de

---

[1] Ibid
[2] AGUILAR SÁNCHEZ (Edwin) Reglas Generales para las Firmas Digitales y Documentos Electrónicos. Op. Cit. p. 10

la sana crítica en donde habrá que tenerse en cuenta cuatro aspectos básicos:

1- La confiabilidad del método con que se haya generado, comunicado o archivado.

2- La confiabilidad del método empleado para conservar su integridad.

3- El método para identificar a la persona que origina el mensaje.

4- Los procedimientos de seguridad empleados.

La Ley Orgánica del Poder Judicial también establece que cuando se den alteraciones que afecten la autenticidad o integridad de los soportes electrónicos, los documentos contenidos perderán su valor jurídico.

También es importante otra norma contenida en dicha Ley que permite la destrucción o reciclaje de expediente, previo archivo o respaldo en "medios electrónicos, informaticos, magnéticos, ópticos, telemáticos o cualquier otro medio con garantía razonables de conservación". [1]

Como podemos notar la Ley autoriza el traslado de la documentación atómica y su archivo en formato electrónico, con la única salvedad de que se garantice la conservación de dichos archivos.

---

[1] Ley Orgánica del Poder Judicial, Artículo 47 bis, adicionado por Ley de Reorganización Judicial.

La Procuraduría General de la República también ha considerado, en cuanto a las labores del Archivo Nacional, que esta institución debe tomar las previsiones del caso con el fin de que los documentos electrónicos tengan el valor jurídico de fuente y constitutivos de medio de prueba, estableciendo las políticas y regulaciones que permitan su recuperación y actualización tecnológicas.[1]

En este sentido, el Archivo Nacional y el Registro Público, cuando registren y archiven documentos electrónicos, en su forma electrónica deben cumplir con tres requisitos fundamentales, que serían:

1- Que el documento sea accesible para su posterior consulta.

2- Que sea conservado en su formato original.

3- Se conserve la información que permita determinar su origen, destino, fecha y hora de creación, envío o recepción.[2]

Para realizar este registro y archivo se debe crear un Registro de Documentos Electrónicos, con personal capacitado para esa labor y para pasar de un formato a otro conforme el avance en la tecnología de archivo y registros electrónicos.

---

[1] Procuraduría General de la República. Dictamen C-283-98

[2] AGUILAR SÁNCHEZ (Edwin) Reglas Generales para las Firmas Digitales y Documentos Electrónicos. Op. Cit. p.17

Por lo anterior podemos concluir que el documento electrónico está plenamente reconocido en nuestra legislación, pero que será con la aprobación de la Ley de Firmas Digitales y Certificados Digitales que en todo sector de la sociedad no habrá duda en equiparar el valor legal del documento firmado digitalmente con el firmado en forma tradicional, tanto en su admisibilidad legal como en su valor de plena prueba.

Asimismo será hasta que se apruebe la ley de firmas digitales que el Notario estará autorizado para incluir dentro de sus funciones, la de dar autenticidad y valor de plena prueba a los actos electrónicos que cumplan con los requisitos de la ley.

Por el momento se ha iniciado un plan de reformas de leyes para adaptarlas al avance de la informativa, como por ejemplo las realizadas en Noviembre del 2001 al Código Penal, que reprime y sanciona delitos como el de la violación y alteración de información contenida en medios informáticos.[1]

[1] Ley #8148, publicada en el Alcance 81 de la Gaceta #216 del 8 de Noviembre del 2001, que adiciona los artículos 196 bis, 217 bis y 229 bis del Código Penal.

CAPÍTULO CUARTO

FUTURA PARTICIPACIÓN DE INSTITUCIONES EN CUANTO AL NOTARIADO DIGITAL.

SECCION I: LA DIRECCIÓN NACIONAL DE NOTARIADO

Con la aprobación de la Ley de Firmas Digitales y Certificados Digitales, algunas instituciones ampliarán sus funciones. Nos interesa únicamente resaltar las que tendrán relación con los Notarios Públicos en su función de autenticar y certificar documentos firmados electrónicamente.

Hemos venido sosteniendo la participación activa del Notario en las Autoridades de Certificación, como parte de la Autoridad de Registro, por ser la persona idónea para identificar a las partes que solicitan los servicios para utilizar firmas digitales.

También serán los únicos que podrán autenticar o certificar una firma digital, cuando una ley requiera que la firma puesta o vinculada a un documento sea autenticada. En este caso la firma digital del Notario debe estar debidamente certificada por una Autoridad Certificante.[1]

Dicho lo anterior surge una interrogante: quién certificará la firma del Notario Público?

---

[1] Así lo establece el artículo 6 del Proyecto de Ley de Firmas y Certificados Digitales. Este artículo actualmente está en revisión por la Comisión Legislativa, la cual está solicitando la participación del Instituto Costarricense de Derecho Notarial.

La respuesta parece muy lógica: La Dirección Nacional de Notariado, por ser la institución a la que le corresponde determinar los medios idóneos de seguridad que deben contener los documentos notariales para que tengan plena validez y la que autoriza a las empresas que suplen dichos medios de seguridad.[1]

La Dirección Nacional de Notariado, sin necesidad de reformar el Código Notarial, dentro de sus atribuciones podrá determinar el uso de la firma digital, el certificado digital, las condiciones de su uso, etc.

Por ser la institución que lleva el registro de firmas de los notarios, sellos blancos y cualquier mecanismo de seguridad que acuerde, sería la entidad idónea para actual como Autoridad Certificadora de los Notarios.

El Master Edwin Aguilar, que actualmente, está asesorando a la Comisión Legislativa encargada del Proyecto de Firmas Digitales y a las instituciones que tendrán relación con los documentos y las firmas electrónicas, me ha expresado que la Lic. Alicia Bogarín Parra le esta solicitando asesoría por su interés en que la Dirección Nacional de Notariado

[1] Código Notarial, artículo 24, inciso n) y ñ).

sea la Autoridad de Certificación de los Notarios, por lo que parece que la lógica se va a aplicar.[1]

SECCION II: EL REGISTRO PUBLICO

Por la seguridad que deben tener los documentos con finalidad de registro, emitidos o autenticados por los Notarios y las Autoridades Judiciales o Administrativas, será el Registro Público el encargado de establecer los mecanismos de seguridad que garanticen la autenticidad de dichos documentos.[2]

Desde Abril de 1979, en nuestro país se puso parcialmente en servicio el sistema de procesamiento de datos para la inscripción de inmuebles por computadora y microfilm.[3]

Desde entonces se ha dado un esfuerzo para lograr la modernización de los sistemas tradicionales de registro y cumplir con los objetivos primordiales de un Registro Inmobiliario cuale son: la seguridad jurídica, la

---

[1] Entrevista con el Msc Edwin Aguilar Sánchez, realizada el 6 de Febrero del 2002.
[2] Ley sobre Inscripción de Documentos en el Registro Público, #3883 del 30 de Marco de 1967, reformada por ley #6145 del 18 de noviembre de 1997, Artículo 5.
[3] LOPEZ-CALLEJA PARIS (Alfredo) La reforma del folio real inmobiliario en Costa Rica. Junta Administrativa del Registro Nacional. Ministerio de Justicia. Costa Rica. 1980. página15.

celeridad en el trámite de inscripción y la facilidad de consulta de la información registral.

Esto se ha logrado con la aplicación de nuevas tecnologías como es la microfilmación y el procesamiento electrónico de datos por ordenadores o computadores. Es por ello que se ha brindado capacitación al personal del Registro y se han adquirido materiales necesarios para el proceso.

Con la implementación de las nuevas tecnologías se ha tratado de conservar la esencia de la estructura del sistema jurídico español, pero introduciendo conceptos como el del Folio Real Alemán "cuyas ideas de unidad de información, brevedad en la transcripción de los asientos y mecanización, son de evidente aceptación por su facilidad de consulta y seguridad."[1]

Además de las ideas alemanas, en nuestro país se tomó como modelo el Registro de Capital Federal de Buenos Aires, Argentina. No obstante nuestra sistema rebasó los conceptos de automatización originarios del Registro Argentino, pues se introdujeron nuevas técnicas que permiten mantener toda la información registral en forma directa para archivos y consultas.[2]

---

[1] LOPEZ-CALLEJA PARIS (Alfredo) Op.cit. p. 21
[2] Ibid. Pp. 22-23

[1] www.registronacional.org.co. Dirección de Informática.
[2] Ley sobre Inscripción de Documentos en el Registro Público, artículos 29 y 31.

Desde entonces nuestro Registro Público se ha desarrollado de tal forma que es uno de los más modernos de América Latina y se ha convertido en el modelo a seguir por los sistemas registrales de otros países.

Actualmente el Registro cuenta con su propia Dirección de Informática cuya labor está orientada al desarrollo de Sistemas de Información y programas laborales en la ejecución de procesos y proyectos difíciles que coadyuvan a facilitar la eficiencia y eficacia de los servicios sustantivos que brinda el Registro Nacional.[1]

Parte de las funciones que le corresponden al Registro Público es corroborar si los medios oficiales de seguridad establecidos por dicha institución y que acompañan a los documentos, corresponden al Notario que lo autoriza[2]. Es por ello que en el futuro, en cuanto a los documentos firmados digitalmente y autorizados por un Notario, el Registro Publico podrá corroborar la firma digital certificada del Notario ante la Autoridad de Certificación Notarial (Dirección Nacional de Notariado).

Además el Reglamento del Registro Público establece que esta institución tiene bajo su competencia las registración y expedición de

[1] www.registronacional.org.co. Dirección de Informática.
[2] Ley sobre Inscripción de Documentos en el Registro Público, artículos 29 y 31.

certificaciones de los registros de sus diferentes secciones, "*valiéndose para ello de las técnicas de microfilmación y cualquier otra tecnología moderna*"[1]

Este Reglamento tiene varias disposiciones mediante las cuales establece que las anotaciones, las inscripciones y el modo de extender las certificaciones se harán por los medios técnicos de computación, microfilmación, digitalización y cualquier otra tecnología que la Dirección del Registro considere más ágiles, eficientes y seguros.[2]

Para esos efectos se dispone que: "*Con el fin de dar la mayor seguridad posible a la información que consta en el Registro y al procedimiento de registración, se podrán crear los sistemas de seguridad que la Dirección considere convenientes.*"[3]

Es por ello que es importante que el Registro adopte estándares de calidad en el archivo de documentos electrónicos, labor que le corresponde a la Dirección de Informática, pues dentro de sus objetivos específicos de trabajo está los de " garantizar seguridad de la información residente en las bases de datos y establecer medidas de seguridad para el uso correcto de los

[1] Reglamento del Registro Público #26771-J, publicado en la Gaceta 54 del 18 de Marzo de 1998, artículo 1.
[2] Reglamente del Registro Público, artículos 28, 29 y 44.
[3] Reglamento del Registro Público, artículo 109.

sistemas de información y los controles de calidad que garanticen el mejoramiento de la productividad ".[1]

Estos estándares de calidad y de seguridad tecnológica serán importantes para la publicidad registral, pues el Registro Público es el que establece la forma de publicitar la información registrada valiéndose de los procedimientos técnicos y tecnológicos que considere seguros y ágiles.

Los asientos registrales generados con base en estos procedimientos, surten con respecto a terceros, los efectos jurídicos derivados de la publicidad registral y tienen la validez y autenticidad que se le otorgan a los documentos públicos.[2]

Es a la Dirección del Registro la que le corresponde determinar la manera en que puede ser consultada la información registral, sin que la misma pueda ser alterada o perdida.[3] En este punto, el Registro Público tiene los mecanismos de seguridad que la tecnología le permite en este momento para la protección de la información registral, la cual deberá actualizar cuando la ley permita el registro de instrumentos públicos electrónicos.

---

[1] www.registronacional.org.co
[2] Ley sobre Inscripción de Documentos en el Registro Público, artículo 32.
[3] Reglamento del Registro Público, artículo 61.

Para que el Registro Público tenga la seguridad necesaria para la inscripción de instrumentos electrónicos y el trasiego de dicha documentación electrónica destinada a su inscripción, deberá establecer un modelo de pirámide de seguridad propia como las enunciadas para las Autoridades de Certificación, con políticas, procedimientos y mecanismos de autenticación, de autorización, encripción y auditoría para el acceso y servicios de la base de datos.

Con base en esa pirámide de seguridad, el Registro podrá determinar quienes pueden ingresar y accesar los datos contenidos en los documentos públicos electrónicos para ser registrados (Notario autorizante y Registrador); además determinará con base en diversos grados de autorización, como lo hace actualmente, hasta donde puede ingresar cada usuario a los servicios y a su base de datos.

Como podemos observar es poca la legislación en cuanto al Registro Público que se debe variar para permitir el registro de instrumentos públicos electrónicos, será por vía reglamentaria que se establecerán los mecanismos necesarios para dicho fin.

Dentro de la adición a las normativas estará la reforma al artículo 57 del Reglamento del Registro que no permite tramitar ningún tipo de documentos por medios postales o tecnológicos.[1]

Con base en la legislación existente para el Registro únicamente será necesaria la implementación de la pirámide de seguridad y la actualización de los medios tecnológicos para iniciar el avance hacia la nueva era de la inscripción de documentos electrónicos.

[1] El artículo 51 del Reglamento del Registro Público dispone expresamente que no se pueden tramitar documentos por medios postales o tecnológicos.

CONCLUSIONES

La red Internet es considerada uno de los cambios revolucionarios más importantes de finales del siglo pasado y es casi impensable el avance que logrará en el presente siglo.

La aparición del Web y la apertura al sector comercial, hizo que la Red pasara a ser parte de la vida de millones de personas y de que cada día el número de usuarios aumente sustancialmente.

Frente a esta expansión del comercio electrónico y la tendencia a nivel mundial de los sistemas legislativos a regular mecanismos probatorios de naturaleza electrónica, resulta necesario que nuestras estructuras normativas se preparen para estos acontecimientos.

El Derecho se encuentra en la necesidad de tutelar el uso de los nuevos recursos tecnológicos y de proteger eficazmente su utilización a través de sistemas que garanticen la autenticidad y seguridad de las transacciones que se producen por vía electrónica.

La realidad avanza con mayor rapidez que el cambio legislativo, pero es necesario atender con rapidez los hechos económicos modernos y efectuar el

marco legal necesario que se ajuste a la realidad económica y al dinamismo que caracteriza a la sociedad en la era del conocimiento.

Los propulsores en nuestro país de la aprobación del Proyecto de Ley sobre Firmas Digitales y Certificados Digitales, dentro de los que se encontraba el anterior Ministro de Ciencia y Tecnología, Guy de Teramond, sufrieron un duro revés al no aprobarse el citado proyecto en la anterior legislatura.

Esperamos que dicha iniciativa encuentre mayor apoyo entre los actuales Diputados, ya que el otorgamiento de validez al uso de las firmas digitales es decisivo para el desarrollo del comercio electrónico en Costa Rica y para poner nuestra legislación en el camino de la era del documento electrónico.

Veamos algunas de las conclusiones establecidas en el desarrollo de este estudio:

a) Hemos analizado como la conceptualización del documento puede ser trasladada al documento electrónico, pues éste cumple con los elementos estructurales y funcionales del documento en general.

La Procuraduría General de la República afirma que por cumplir con los requisitos de formación y seguridad de los documentos, no existe inconveniente en considerar el documento electrónico como documento escrito.

En nuestro país la ley admite y da validez a los documentos electrónicos, lo que no existe es una disposición que le otorgue plena fuerza probatoria, pues deberá acompañarse con todo tipo de prueba para darle sustento legal.

Es por ello que para lograr una equiparación total, a efecto de darle plena validez legal y probatoria, es necesaria la aprobación de una ley que así lo establezca.

b) Se analizó toda la problemática de la autorización de documentos notariales otorgados en el extranjero, tanto por los Cónsules de nuestro país en el exterior, como por los Notarios Públicos en su actuación extraterritorial. Esta práctica encarece el otorgamiento de actos y contratos cuyos efectos deban tener efectos en Costa Rica y entorpece la celeridad que se requiere hoy día en el mundo globalizado.

Es por ello que es necesaria la aprobación de las firmas y los certificados digitales, pues ello conllevaría una celeridad en el otorgamiento de documentos y una merma en los costos por traslados a los Consulados o de los Notarios nacionales al extranjero, al poder el Notario certificar directamente la autenticidad e integridad del acto realizado electrónicamente.

c) Para lo anterior es necesaria la firma digital, la cual surge de un proceso que utiliza técnicas de criptografía de llave pública y una función matemática con

la cual se verifica que el emisor de un mensaje está en posesión de una única llave privada y además verifica que el mensaje no ha sido alterado en tránsito.

La firma digital es tan o más segura que la firma ológrafa, pues además de tener más elementos es inimitable. La firma digital cambia con cada texto.

Firmar digitalmente un documento electrónico tiene los siguientes propósitos fundamentales: 1) Garantiza su autenticidad, ya que se reconoce que determinada persona es el autor del documento o acepta como suyo el contenido del mismo. 2) Garantiza su confiabilidad, pues el documento es inaccesible a terceros no autorizados. 3) Garantiza la integridad de su contenido después de la firma, pues si un documento es alterado en el transcurso de su envío o recepción, es detectado inmediatamente. 4) Garantiza el no repudio, pues ninguna de las partes en una transacción electrónica puede negar haber recibido un documento electrónico.

Tenemos que dejar claro que un documento firmado digitalmente no es técnicamente un documento firmado en forma escrita, sino que es un sello electrónico equivalente funcionalmente a una firma.

d) El funcionamiento global de esta tecnología está apoyado y supervisado por una tercera parte confiable denominadas: Autoridades de Certificación.

En la economía digital y dentro de la infraestructura de llave pública, son las autoridades certificadoras las encargadas de actuar como terceros de confianza, promoviéndose como entes seguros y confiables. El único interés de estos empresas será el de brindar las herramientas necesarias para que las transacciones de los usuarios sean seguras y privadas.

Estas autoridades de certificación atestiguan, mediante un Certificado Digital, la titularidad e identidad de una clave pública con una persona física o jurídica, realizando una autenticación del usuario del sistema.

Esta autenticación digital establece la confianza en las transacciones y no debe ser confundida con la autenticación legal, que en nuestro ordenamiento está reservada para los Abogados y Notarios. Esta posición es la que prevalece, pues las corrientes doctrinales predominantes y los ordenamientos de distintos países (incluyendo el Proyecto de Ley nacional) establecen que cuando la ley requiere una autenticación notarial, será necesario que un Notario estampe su firma digital en asocio con la firma que se autentica.

La discusión de la invasión de competencias notariales de las Autoridades de Certificación está superada, pues únicamente mediante ley se puede depositar la fe pública en personas distintas a los Notarios Públicos.

e) Es precisamente en este punto, donde comienza la discusión de la actividad de la función notarial en relación con las nuevas tecnologías en la creación de documentos y la firma de los mismos.

Algunas posiciones han tratado de armonizar los principios clásicos de la función notarial, con los avances tecnológicos en la elaboración de documentación electrónica.

Esto no es posible, ya que dichos principios deben ser superados, como por ejemplo, el de la "unidad del acto" como unidad temporal y espacial propia de la expresión del consentimiento contractual. Únicamente queda inalterable la expresión del consentimiento en un solo documento, dando lugar a la que se denomina: "unidad de texto".

La labor notarial tendrá un nuevo campo de acción de su función en la contratación y actuación electrónica, por varios aspectos:

Primero y siguiendo la corriente actual, será el funcionario encargado de autenticar y dar fe de la identidad y capacidad de los usuarios ante las Autoridades Certificadoras y de Registro, trasladando la identificación tradicional de los documentos oficiales a los medios electrónicos de identificación.

Como otra función a realizar, el Notario podrá certificar las firmas digitales de documentos electrónicos privados.

La participación del Notario en la transacción, ejercería un reconocimiento del control de legalidad para la validez del contenido jurídico del negocio y un control sobre la seguridad tecnológica de dicha transacción, pues la misma quedaría asentada en matrices electrónicas bajo la custodia del Notario.

El rol del Notario en la contratación y actuación electrónica es primordial en el sustento de la legalidad de los procesos de certificación digital, pues traslada al mundo virtual la fe pública que ejerce en el mundo real.

Aunado a esto, ya indicamos que siempre que se requiera un documento con autenticación legal, será la firma digital de un Notario Público la que garantizará la integridad y el origen del mensaje.

f) Para realizar la función notarial en el ámbito electrónico, el Notario debera estar capacitado para otorgar ese servicio, dando nacimiento a la figura del "Cibernotario o Notario Cibernético".

Este deberá ser una persona habilitada para ejercer la profesión notarial y contar con la capacitación para adquirir conocimientos suficientes en informática y como certificar digitalmente, debidamente comprobada ante la Dirección

Nacional de Notariado; además, por supuesto, debe contar con el equipo necesario.

El Notario Cibernético debe actualizarse en sistemas informáticos, para mantener vigente su licencia o permiso.

g) En el momento en que se apruebe el uso de las firmas digitales y que el Notario pueda iniciar a ejercer sus funciones por medios electrónicos, podemos comenzar a visualizar la posibilidad del Protocolo Digital.

Hemos analizado la viabilidad de dicho instrumento de archivo y conservación de documentos electrónicos, bajo la custodia del Notario y de alguna Autoridad como el Archivo Nacional.

Los especialistas analizan que dicho Protocolo tendría las mismas características que el protocolo de papel, con la única diferencia que no es atómico y que solamente se debe enseñar a los Notarios las técnicas de archivo digital.

Debemos de aprovechar la discusión que sobre estos temas se han realizado en países donde se han aprobado leyes sobre firmas digitales y la participación de los Notarios en el sistema, para aplicar lo que corresponda a nuestro ordenamiento.

h) Es interesante analizar como nuestra legislación se le han ido introduciendo normas que permiten el uso de documentos electrónicos con plena validez y eficacia legal.

Así vemos como nuestros Tribunales de Justicia, la Administración Central y entidades como el Colegio de Abogados la Defensoría de Habitantes, utilizan los medios electrónicos para realizar notificaciones.

El avance del análisis del tema en el campo judicial es tan importante, que en el proyecto de Código Procesal General se ha previsto la utilización de los documentos electrónicos y firmas digitales para hacer realidad el procedimiento electrónico.

i) La Procuraduría General de la República dictaminó que solo por creación de ley es posible el reconocimiento con valor jurídico de la combinación de caracteres electrónicos utilizados como firmas, pensando en una ley de firmas digitales. Pero lo cierto es que existen leyes y reglamentos, que individualmente han venido autorizando la utilización de ciertos elementos electrónicos de seguridad para ser utilizados como firma de un documento electrónico.

Está práctica no es saludable, pues como expresa el Master Christian Hess, se debe evitar legislar sobre firma digital a partir de sus aplicaciones en algunas áreas, sino garantizar una apertura a todos los sectores de la sociedad civil.

j) Cuando se apruebe la Ley de Firmas y Certificados Digitales, será necesario ir delineando la función de la Dirección Nacional de Notariado, como institución que determinará el uso de la firma digital dentro de los medios idóneos para otorgar seguridad a los documentos notariales electrónicos.

Por su parte el Registro Público únicamente deberá reformar el artículo 57 de su Reglamento, para que se le permita tramitar documentos por medios tecnológicos.

Nuestra intención con el desarrollo de este tema, fue mostrar un poco la realidad del avance en la tecnología, la insuficiencia de nuestro ordenamiento, la soluciones encaminadas en otros países y la necesidad de legislar sobre firma digital.

Esperamos que apruebe pronto la regulación de un mecanismo necesario para nuestra realidad social, ya que como hemos sostenido se debe adecuar nuestra legislación a los cambios sociales influenciados por el avance en la tecnología.

Por otra lado, no debemos esperar que sea por jurisprudencia que se implemente la validez del uso de los documentos electrónicos como pruebas en juicio, para luego tomar conciencia de la necesidad de legislar en ese sentido.

Nuestros legisladores tienen la imperiosa necesidad de aprobar la ley necesaria para reglar los relativo al documento informático y la firma digital. Con ello se desarrollaría sus potenciales aplicaciones que van más allá del comercio electrónico, pues resultaría vital para avances como el del notariado electrónico.

BIBLIOGRAFÍA

REVISTAS

1- AXELRUD DE LENDNER, Rosa M, Notarialización Electrónica, en Revista Internacional del Notariado, N°96, segundo semestre, año 1998, ONPI, Buenos Aires, Argentina.

2- AXELRUD DE LENDNER, Rosa M, Las llaves, en Revista Internacional de Notariado, N°96, segundo semestre, ONPI, Buenos Aires, Argentina, 1998.

3- BARASSI, Theodore, The Cybernotary, en Revista Notarius Internacional, Vol.1, N°3, 1996, KluwerLaw International, Holanda.

4- Comentario sobre el proyecto de Ley Chileno del Documento Electrónico, en Revista Internacional de Notariado, N°93, primer semestre, ONPI, Buenos Aires, Argentina., 1997.

5- DE LA FUENTE (Juan Ángel) La Contratación Electrónica, la Criptografía y la Firma Digital, en Revista Internacional del Notariado, ONPI, Buenos Aires, N° 96, Segundo Semestre, 1998.

6- Documento Electrónico en Italia, Revista Internacional del Notariado, N°94, segundo semestre, ONPI, Buenos Aires, Argentina, 1997.

7- El Documento informático y la seguridad jurídica, en Revista ANOTA, N°4, mayo, año 6, Asociación de Notarios de Puerto Rico, San Juan, Puerto Rico, 1992.

8- HACKENBUCHNER, Wolfang, Nacimiento del Ciber-Notario, extracto de la Revista Nota Bene, N°22, en Revista Internacional del Notariado, N°94, segundo semestre, ONPI, Buenos Aires, Argentina, 1997.

9- Informe de la K:N:B: sobre el "Notario y el acuerdo jurídico electrónico en Holanda", en Revista Internacional de Notariado, N°93, primer semestre, ONPÍ, Buenos Aires, Argentina, 1997.

10- KEMPER, Ana María. Seguridad Jurídica en la contratación por medios electrónicos, 24° Jornada Notarial Argentin, en Revista ANOTA, N°3, año 11, Asociación de Notarios de Puerto Rico, San Juan, Puerto Rico, 1995.

11- KENNAIR, William B. El Concepto y el Desarrollo del "Cybernotary", en Boletín de la Comisión de Asuntos Americanos, Unión Internacional del Notariado Latino, Año VII, N°27, Santo Domingo, República Dominicana, 1998.

12- LAMBERT, Jean. Le Secret Profesionnel et communications électroniques: Prenez Garde, en Revista Notarius International, Vol., N°24, Kluwer Law International, Holanda, 1997.

13- MARRERO, Angel R. El Notario Cibernético, en Revista ANOTA, N°4, año 9, Abril-Mayo, Asociación de Notarios de Puerto Rico, San Juan, Puerto Rico, 1996.

14- MARRERO, Angel R. El Notario Anglosajón, en Revista ANOTA N°2, año 10, Abril-Mayo, Asociación de Notarios de Puerto Rico, San Juan, Puerto Rico, 1996.

15- MICCOLI, Mario. Cybernotary, Revista Internacional del Notariado, N°91, primer semestre, ONPI, Buenos Aires, Argentina, 1995.

16- MURRIETA, Katia. La Contratación Electrónica, en Boletín de Comisión de Asunto Americanos, Unión Internacional del Notariado Latino, Año VII, N°28, Santo Domingo, República Dominicana, 1999.

17- Nacimiento del Ciber-Notario. Revista Internacional de Notariado, N° 94, ONPI,Buenos Aires, Segundo Semestre, año 1997, p-104., extracto de la Revista NOTA BENE del 22 de Agosto de 1996.

18- RUPLEY (Sebastián) La Guerra del Web. PC Magazine en español. Documento sin año,1997.

19- Sexta Jornada de Derecho Notarial del Norte, Centroamérica y el Caribe, "La informática en el Quehacer del Notario". Tegucigalpa, Honduras, Mayo,

1995, en Revista ANOTA, N°4, año 6, Asociación de Notarios de Puerto Rico, San Juan, Puerto Rico.

20- Vía Internet (Revista) Año 1, número 1, San José, Agosto del 1997.

21- WEYTS, Valerie et Luc. Du Notarie classique au Notarie electronique. Revista Notarius International, Vol. L, N°3, 1996, Kluwer Law International, Holanda.

REVISTAS ELECTRÓNICAS

22- ARCE (Alfonso José) DIAZ LANNES (Federico Santiago) La Firma Digital. Aspectos Jurídicos. Su aplicación a las Comunicaciones Previstas por la Ley #22.172, 1979, Revistas Electrónica de Derecho Informático. www.publicaciones.derecho.org/redi.

23- BARZALLO (José Luis) Ecuador: Los Terceros de Confianza en el Comercio Electrónico. Revista Electrónica de Derecho Informático, #33, www. publicacionesderecho. Org/redi. Abril, 2001.

24- CARRASCO BLANC (Humberto) Aspectos de la formación del consentimiento electrónico. 1999. Revista Electrónica de Derecho Informático. www.publicaciones.derecho.org/redi

25- CORNEJO LOPEZ (Valentino). Una realidad Mexicana, la Firma Electrónica y la Participación del Notario Mexicano. Revista Electrónica de Derecho Arbor, Agosto, 2000. **www.derecho.org.v/lex.com.**

26- CORNEJO LOPEZ (Valentino) Testigos Electrónicos ante la Dificultad de la Contratación Electrónica en el Derecho Mexicano. Revista Electrónica de Derecho Arbor, 2000. **www.derecho.org.v/lex.com.**

27- DEVOTO (Mauricio). El Dinero Electrónico y el Lavado de Dinero. Revista Electrónica de Derecho Informático, 1998. **www.publicaciones.derecho.org**

28- GAETE GONZALEZ (Eugenio Alberto) Documento Electrónico e Instrumento Público. Revista Electrónica de Derecho Informático, Nº 24, Julio, 2000, en **www.derecho.org.v/lex.com**

29- GAETE GONZALEZ (Eugenio) Firma Electrónica y Firma Digital, 2001. Documento enviado por el Dr. Gaete adjunto a mensaje de correo electrónico dirigido a Kadir Cortés Pérez el 10-02-2002.

30- GONZALEZ T. (Patricio) VILLALÓN I. (Álvaro). Introducción a la Criptografía. Revista Electrónica de Derecho Informático. 1999. **www.derecho.org**

31- GORDO SAEZ (Roberto). La transmisión de información en Internet. http// **www.bachillerato.uchile.cl**, 1998.

32- Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre el Comercio Electrónico. www.uncitral.org.

33- HESS ARAYA (Christian) Comentarios al proyecto de Ley de Firma Digital de Costa Rica, enviado al Dr. Luis Paulino Mora, Presidente de la Cortes Suprema de Justicia, el 19 de Febrero del 2001, www.comunidad.derecho.org/chess

34- Historia de Internet. www,flash.net/ hejrusso/historia.htm.

35- IRIARTE AHON (Erick) Firma Digital y Certificado Digital. El Proyecto Peruano. Revista Electrónica de Derecho Informático, 1999. www.publicaciones.derecho.org/redi.

36- JIJENA LEIVA (Renato Javier), Comercio Electrónico y Derecho. La problemática jurídica del Comercio Electrónico. Universidad Católica de Valparaíso, 1.999. Documento sin numeración, http://publicaciones. derecho.org/redi/.

37- JIJENA LEIVA (Renato) Internet Certificada. www. acerita.com, Abril, 2001.

38- LEAL NERY (Hugo) El Protocolo del Cibernético Revista Electrónica de Derecho Informatico.N° 33 Abril, 2001. **www. acertia.com**

39- LOPEZ CEBADA (Juan Jesús) Breves Consideraciones sobre las Posibilidades Subyacentes en la Firma Electrónica Avanzada, 1999, España.

En Revista Electrónica de Derecho Informático, www.publicaciones.derecho.org/

40- MAESTRE (Javier A.) El empleo de la Firma Electrónica en el Sistema Registral Español.: Comentario a la Resolución de la Dirección General de los Registros y del Notariado, de 26 de abril de 2000. Revista Electrónica de Derecho Informático. www.publicacionesderecho.org/redi

41- MARTÍN REYES (María de los Angeles) el documento y la firma electrónica. Nuevas perspectivas en la contratación. Revista Electrónica de Derecho Informático. 1999. ww.publicaciones.derecho.org/redi.

42- Mensaje de correo electrónico dirigido por el Dr. Eugenio Gaete a Hugo Leal Neri, el 29 de Diciembre del 2001.

43- Mensaje de correo electrónico dirigido por el Dr. Eugenio Gaete a Kadir Cortés Pérez el 29 de Diciembre del 200.

44- MIRAVET BONET (Juan Salvador). Protocolos TCP/IP. **Al019803@alumail.uji.es**, 1999.

45- MUÑOZ ESQUIVEL (Oliver) Actividad de las Entidades de Certificación frente a la Función Notarial, www.publicaciones.derecho.org/redi, #25 15 de Junio , 2000.

46- MUÑOZ TORRES (Ivonne Valeria) Efectos Reales mas no legales de las reformas legislativas en materia de comercio electrónico: La situación del Notario Público. 1997-2000. Artículo en sitio www.acertia.com

47- PEREZ MERAYO (Guillermo). La Informática y la Política. Hacia un Gobierno Electrónico. Revista Electrónica de Derecho Informatico, www.derecho .org Febrero, 2000.

48- PEREZ PEREIRA (Maria) Hacia la seguridad en el Comercio Electrónico. Revistade Derecho Informático, 1999, www.publicaciones.derecho.org/redi.

49- RAMOS SUAREZ (Fernando) Eficacia Jurídica de una Transacción electrónica. La figura del No Repudio. www.publicaciones.derecho.org./redi.

50- RAMOS SUAREZ (Fernando) La Firma Electrónica. Revista Electrónica de Derecho Informático. 2000. www.publicaciones.derecho.org/redi.

51- RAMOS SUAREZ (Fernando). Protocolo SET. Revista Electrónica de Derecho Informático. **www.derecho.org**.

52- RAMOS SUAREZ(Fernando) Como aplicar la nueva normativa sobre Firma Electrónica. www.legalia.com

53- RIBAS (Xavier) Propuestas de Directiva sobre Firmas Electrónicas. Revista Electrónica de Derecho Informático, 1999, www.publicaciones.derecho.org/redi

54- RICO CARRILLO (Mariliana) La oferta y la aceptación en la contratación electrónica. 1997-2000. Revista Electrónica de Derecho Informático. www.publicaciones.derecho.org/redi

55- SANDOVAL LOPEZ (Ricardo) Comentarios Sobre el Proyecto Relativo al Documento y Firmas Electrónicas, 1999, www.publicaciones.derecho.org/redi.

56- PEREZ PEREIRA (María) Hacia la seguridad en el Comercio Electrónico. Revista Electrónica de Derecho Informático. www.publicacione.derecho.org.

57- SEGURA LOARTE (Alejandro) Hacia el establecimiento del documento digital en el Perú. Revista electrónica de Derecho Informático. www.publicacionesdereco.org/redi.

58- SOTO BORJA Y ANDA (Ignacio) La Fe pública Notarial para el Comercio Electrónico. 1997. www.acertia.com.

59- VELARDE KOECHLIN (Carmen) El Fedatario Particular Juramentado en Informática: Institución Peruana al Servicio de una solución Global, 2000, www.publicaciones.derecho.org/redi.

60- **www. acertia.com** El Rol del Federatario en la Economía Digital, documento sin autor y sin numeración de página.

61- www.isoc.org/internet/history/brief.htm

62- www. la nación.com Reportaje Juan Fernando Lara, Búsqueda fácil en internet.

63- **www.notariadomexicano.org.m**

64- **www.jupiter.com**, en referencia a los servicios de planificación de estrategias (SPS- Strategic Planning Services)

65- www.registronacional.go.cr, sitio del Registro Nacional en Internet.

CODIGOS, LEYES, REGLAMENTOS Y DIRECTRICES

66- Código Aduanero Uniforme Centroamericano (CAUCA III) Nº 29046-COMEX, del 20 de Octubre del 2000

67- Código Civil. Colección Leyes. Editorial Porvenir, 12ª. Edición, San José, 1998.

68- Código de Comercio y sus reformas, Ley #3284, Edición Electrónica de Sistemas Legales Master Lex, 1964.

69- Código de Normas y Procedimientos Tributarios. # 4755, del 29 de Abril de 1971, publicado en el Alcance 567 de la Gaceta 117 del 4 de Junio de 1971.

70- Código Procesal Civil, Sétima Edición, San José. Editorial Investigaciones Jurídicas, S.A. 1.999.

71- Código Notarial. Ley 7774 del 22 de mayo de 1.998. San José, Editorial Investigaciones Jurídicas S.A., Primera Edición, Edición concordada por el Lic. Herman Mora, julio del 2.000.

72- Convención de Viena Sobre Relaciones Consulares, Ley #3767 del 3 de Noviembre de 1966.

73- Directriz #003-98, de la Dirección Nacional de Notariado, de las 10 horas 30 minutos del 24 de noviembre e 1998.

74- Directriz número 626-1999, de la Dirección Nacional de Notariado, de las 7:33 horas del 20 de Julio de 1999.

75- Exposición de motivos de la Directiva del Parlamento Europeo y del Consejo 1999/93/CE del 13 de diciembre de 1999, en la que se establece un marco comunitario para la firma electrónica.

76- Ley de Contratación Administrativa 7494 del 2 de Mayo de 1995, publicada en el Alcance 20 de la Gaceta 120 del 8 de Junio de 1995.

77- Ley General de Aduanas. # 7557, del 20 de Octubre de 1995 publicado en la Gaceta 212 del 8 de Noviembre de 1995.

78- Ley General de Tránsito por vías públicas terrestres, #7331 del 13 de Abril de 1993, reformada con la vigencia del Código Notarial en el año 1998.

79- Ley Orgánica del Poder Judicial, # 7333, Edición Electrónica de Sistemas Legales Master Lex, 1993.

80- Ley Orgánica del Servicio Consular, #46 del 7 de Junio de 1925.

81- Ley Reguladora del Mercado de Valores, #7732 del 17 de Diciembre de 1997, publicado en la Gaceta #18 del 27 de Enero de 1998.

82- Ley de Registro, Secuestro y examen de documentos privados e intervención de las comunicaciones, #7425 del 09 de Agosto de 1994.

83- Ley #8148, publicada en el Alcance 81 de la Gaceta #216 del 8 de Noviembre del 2001, que adiciona los artículos 196 bis, 217 bis y 229 bis del Código Penal.

84- Ley sobre Inscripción de Documentos en el Registro Público, #3883 del 30 de Marco de 1967, reformada por ley #6145 del 18 de noviembre de 1997.

85- Ley Modelo de la CNUDMI sobre Comercio Electrónico, en www.uncitral.org

86- Procuraduría General de la República, Dictamen C-283-98, dirigida al Archivo nacional el 24 de Diciembre de 1998.

87- Proyecto de Ley de Firmas Digitales y Certificados Digitales, del 22 de Febrero del 2001, Expediente #14276 de la Asamblea Legislativa.

88- Directiva 97/66/Ce del 15 de diciembre de 1997, del Parlamento Europeo y del Consejo, relativa al Tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

89- Directiva 97/7/CE del Parlamento Europeo y del Consejo del 20 de Mayo de 1997, relativa a la Protección de los Consumidores en materia de contratos a Distancia.

90- Directiva del Parlamento Europeo y del Consejo del 24 de Octubre de 1995, sobre el tratamiento de datos personales y su libre circulación.

91- Directiva del Parlamento Europeo y del Consejo 2000/31/CE del 8 de Junio del 2000.

92- Propuesta de Directiva del Parlamento Europeo y del Consejo 98/0245, del 19 de Noviembre de 1998.

93- Reglamento a la Ley General de Aduanas, Decreto 25270-H del 14 de Junio de 1996, reformado por Decreto 28976-H del 27 de Setiembre del 2000.

94- Reglamento del Registro Público #26771-J, publicado en la Gaceta 54 del 18 de Marzo de 1998.

95- Reglamento General de la Contratación Administrativa, #25038-

96- Reglamento de Notificaciones y Comunicaciones por medios Electrónicos , # 15-2000.

97- Reglamento de Procedimiento interno en trámite de quejas ante la Fiscalía del Colegio de Abogados de Costa Rica, Sesión # 12-99, 1999.

98- Reglamento de la Defensoría de los Habitantes, #22266-J, 1993.

TRATADOS Y TESIS

99- AGUILAR SÁNCHEZ (Edwin). El Comercio Electrónico. Curso de Nivel Superior sobre Comercio Electrónico. Instituto Costarricense de Administración Pública, San José, Enero-Febrero, 2000.

100- AGUILAR SÁNCHEZ (Edwin).Economía Digital. Curso de Nivel Superior, impartido en el Instituto Centroamericano de Administración Pública, ICAP, San José, Enero-Febrero, 2000.

101- AGUILAR SÁNCHEZ (Edwin) Reglas Generales para las Firmas, Certificados y contratos Digitales, Seminario de Notariado Digital, Registro Público de la Propiedad, 2001.

102- AGUILAR SÁNCHEZ (Edwin) Seguridad y Privacidad en las Transacciones Digitales. Seminario de Notariado Digital, Registro Público, 2001.

103- ALCOLEA (José Miguel) La Incorporación de las técnicas electrónicas, informáticas y telemáticas a la actividad de la Administración del Estado Español. Derecho de Internet. Contratación electrónica y firma digital. España. Editorial Aranzadi S.A., 1° edición, 2000.

104- ALONSO UREBA (Alberto) ALCOVER GARAU (Guillermo) La Firma Electrónica. Derecho de Internet, Contratación Electrónica y Firma Digital. España, Editorial Aranzadi S.A. 1ª. Edición, 2000

105- BARRIUSO RUIZ (Carlos), La contratación electrónica, Madrid, Editorial Dykinson S.L., Primera Edición, 1.998.

106- BOGARIN NAVARRO (Rodrigo) Descubra el mundo de Internet, San José, Costa Rica, Editorial Tecnológica de Costa Rica, 1era. Edición, 1995.

107- CAMARGO, Pedro Pablo. Tratado de Derecho Internacional, tomado de la Antología de Lecturas de Derecho Internacional Público I, Facultad de Derecho, Universidad de Costa Rica, 1998.

108- CERVELLO GRANDE (José Maria) La prueba y el documento electrónico. Derecho de Internet, Contratación electrónica y firma digital. España, Editorial Aranzadi S.A., 1° Edición, 2000.

109- COMER (Douglas E.) El libro de Internet, México, Editorial Prentice-Hall, Segunda Edición, 1.998.

110- COMER (Douglas E.) Introducción al Estudio del TCP/IP, Prentice-Hall, México, 1997.

111- CRUZ CIENFUEGOS, Jorge Ernesto. La Función Notarial en el Servicio Exterior, su regulación en los países centroamericanos y particularmente en el Derecho salvadoreño y costarricense, Facultad de Derecho, Universidad de Costa Rica, 1979.

112- Enciclopedia Autodidáctica Interactiva Océano, Volumen 6, Océano Grupo Editorial S.A. Barcelona, 2000.

113- GIMÉNEZ ARNAU (Enrique) Derecho Notarial. Pamplona. Ediciones Universidad de Navarra, Segunda Edición, 1976.

114- GONZALEZ (Carlos E.) Derecho Notarial. La Ley Sociedad Anónima Editora e Impresora, Buenos Aires, Argentina, 1.971..

115- GONZALEZ -ECHENIQUE CASTELLANOS DE UBAO (Leopoldo). Estudios de la Directiva y del Decreto ley de 17 de Septiembre de 1999, sobre Firma Electrónica. Derecho de Internet, Contratación Electrónica y Firma Digital. España, Editorial Aranzadi S.A. 1ª. Edición, 2000.

116- HERRERA DURAN (RITA) y VILLALOBOS SOTO (JOAQUIN) Derecho Consular Costarricense. Tesis para optar al título de Licenciados en derecho. Facultad de Derecho. Universidad de Costa Rica, 1983.

117- KNORR BRICEÑO (Jolene Marie) y ROLDAN SAUMA (Marcelo), La Protección del Consumidor en el Comercio Electrónico, Costa Rica, Editorial Investigaciones Jurídicas S.A., Primera Edición, 2.001.

118- LARRAUD (Rufino), Curso de Derecho Notarial, Editorial Depalma, Buenos Aires, 1976.

119- LOPEZ-CALLEJA PARIS (Alfredo) La Reforma del Folio Real Inmobiliario en Costa Rica. Junta Administrativa del Registro Nacional, Ministerio de Justicia, Costa Rica, Primera Edición, 1980.

120- MATEU DE ROS (Rafael) El consentimiento y el Proceso de Contratación Electrónica. Derecho de Internet. Contratación electrónica y firma digital, España, Editorial Aranzadi S.A., 1° Edición, 2000.

121- MARTINEZ NAVARRETE (Doroteo) El Documento Público Notarial, Tesis para obtar al grado de Licenciatura en Derecho, Facultad de Derecho Universidad de Costa Rica, 1980.

122- MORA VARGAS (Herman) Manual de Derecho Notarial: La Función Notarial, Editorial Investigaciones Jurídicas S.A., Primera Edición, San José, 1999.

123- Océano Uno Color, Diccionario Enciclopédico, Océano Grupo Editorial S.A., Barcelona, Edición 1998.

124- PALLARES, Eduardo. Diccionario de Derecho Procesal Civil. México. Editorial Porrúa S.A. Edición décimo sexta. 1.984.

125- PELOSI, Carlos. El documento notarial. Buenos Aires. Editorial Astrea de Alfredo y Ricardo de Palma. 1992.

126- RECORDER DE CASSO (Emilio) Algunas Observaciones en torno a contratos, electrónica y fe pública. Derecho de Internet. Contratación electrónica y firma digital. . España, Editorial Aranzadi S.A. 1ª. Edición, 2000.

127- RIBAS ALEJANDRO (Javier) Aspectos Jurídicos del Comercio Electrónico en Internet, España, Editorial Aranzadi, 1° edición, 2000.

128- RUIZ-GALLARDON (Miguel) Fe Pública y Contratación Telemática. Derecho de Internet. Contratación electrónica y firma digital. España, Editorial Aranzadi S.A. 1ª. Edición, 2000.

ANEXOS

LEY MODELO DE LA CNUDMI SOBRE LAS FIRMAS ELECTRÓNICAS

2001

(Extracto del informe de la Comisión de las Naciones Unidas sobre el Derecho Mercantil Internacional sobre la labor de su trigésimo cuarto período de sesiones, celebrado en Viena, desde el 25 de junio al 13 de julio de 2001. El texto de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas fue adoptado el 5 de julio de 2001 [Nota: la versión final de la Guía para la incorporación al derecho interno de la Ley Modelo será publicada durante el segundo semestre del año 2001])

Anexo II

Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001)

Artículo 1
Ámbito de aplicación

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No derogará ninguna norma jurídica destinada a la protección del consumidor.

---

* La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

"La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [ ]."

** El término "comercial" deberá ser interpretado en forma lata de manera que abarque las cuestiones que dimanen de toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, aunque no exclusivamente, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje ("factoring"); arrendamiento con opción de compra ("leasing"); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera.

Artículo 2
Definiciones

Para los fines de la presente Ley:

a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al

mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos;

b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;

c) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

d) Por "firmante" se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa;

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

f) Por "parte que confía" se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Artículo 3
Igualdad de tratamiento de las tecnologías para la firma

Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

Artículo 4
Interpretación

1. En la interpretación de la presente Ley se tendrán en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y de asegurar la observancia de la buena fe.

2. Las cuestiones relativas a las materias que se rigen por la presente Ley que no estén expresamente resueltas en ella se dirimirán de conformidad con los principios generales en los que se basa esta Ley.

Artículo 5
Modificación mediante acuerdo

Las partes podrán establecer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 6
Cumplimiento del requisito de firma

1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.

2. El párrafo 1) será aplicable tanto si el requisito a que se refiere está expresado en forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3. La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1) si:

a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

4. Lo dispuesto en el párrafo 3) se entenderá sin perjuicio de la posibilidad de que cualquier persona:

a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1), la fiabilidad de una firma electrónica; o

b) aduzca pruebas de que una firma electrónica no es fiable.

5. Lo dispuesto en el presente artículo no será aplicable a: [Y].

Artículo 7
Cumplimiento de lo dispuesto en el artículo 6

1. [*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia*] podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6 de la presente Ley.

2. La determinación que se haga con arreglo al párrafo 1) deberá ser compatible con las normas o criterios internacionales reconocidos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 8
Proceder del firmante

1. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme al artículo 9 de la presente Ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:

i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.

2. Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1).

Artículo 9
Proceder del prestador de servicios de certificación

1. Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales;

c) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

i) el método utilizado para comprobar la identidad del firmante;

ii) cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8 de la presente Ley;

vi) si se ofrece un servicio para revocar oportunamente el certificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 de la presente Ley y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que existe un servicio para revocar oportunamente elcertificado;

f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.

2. Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1).

Artículo 10
Fiabilidad

A los efectos del apartado f) del párrafo 1) del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) los recursos humanos y financieros, incluida la existencia de activos;

b) la calidad de los sistemas de equipo y programas informáticos;

c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;

e) la periodicidad y el alcance de la auditoría realizada por un órgano independiente;

f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; o

g) cualesquiera otros factores pertinentes.

Artículo 11
Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

a) verificar la fiabilidad de la firma electrónica; o

b) cuando la firma electrónica esté refrendada por un certificado:

i) verificar la validez, suspensión o revocación del certificado; y

ii) tener en cuenta cualquier limitación en relación con el certificado.

Artículo 12
Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras

1. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:

a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni

b) el lugar en que se encuentre el establecimiento del expedidor o del firmante.

2. Todo certificado expedido fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que todo certificado expedido en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.

3. Toda firma electrónica creada o utilizada fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que toda firma electrónica creada o utilizada en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.

4. A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de párrafo 2), o del párrafo 3), se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5. Cuando, sin perjuicio de lo dispuesto en los párrafos 2), 3) y 4), las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.

PROYECTO DE LEY

LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES

Expediente N° 14.276

ASAMBLEA LEGISLATIVA:

La comunicación entre los seres humanos, particularmente las comunicaciones a distancia se han facilitado conforme avanza la tecnología. El telégrafo, el teléfono, la radio, la televisión, el fax, cada uno a su tiempo, han representado importantes pasos en materia de comunicación humana, y han conformado una base tecnológica de mucha capacidad, la cual ha iniciado una verdadera revolución en las comunicaciones y el desarrollo de las sociedades contemporáneas. Una de las áreas más beneficiadas con estas nuevas y ágiles herramientas de comunicación es la del comercio. Por su misma naturaleza, requiere cada vez más de mecanismos ágiles y eficientes pero también seguros de comunicación.

Esta cadena de logros tecnológicos en materia de comunicación ha alcanzado un punto muy alto con la extensión de la red internacional o Internet (red de redes), la cual ha ampliado exponencialmente las posibilidades y facilidades de comunicación entre los seres humanos. Es, definitivamente, un medio que no puede ser ignorado por ninguna persona, mucho menos por el sector comercial alrededor de todo el orbe. Y en efecto, no lo ha sido. Los expertos coinciden en afirmar que la Sociedad de la Información ha encontrado en Internet el canal de flujo ideal, por sus preciados atributos: rápido, barato, y cada vez más extendido y eficiente. Cada vez más empresas deciden incursionar en el mercado

virtual, y basan sus comunicaciones externas en ella; igualmente, con más pausa y mesura pero con la misma decisión, los operadores financieros comienzan a utilizar el nuevo medio. Y no podría ser de otra forma ya que en el mercado virtual adquieren ventajas comparativas que sencillamente no existen en el mundo físico, siendo la reducción de costos uno de sus principales beneficios. Es notable que este tipo de instrumento accesible actualmente a una parte de la población, era accesible hasta hace pocos años, únicamente a las corporaciones más poderosas del planeta. La pequeña y mediana empresa ven en efecto en la Internet la posibilidad de un acceso sin precedentes a la información y los mercados mundiales a un costo reducido, y con tendencia a bajar, no a subir, a medida que la red de redes se extiende en todo el orbe. Estamos presenciando una verdadera revolución en el acceso al conocimiento, a la información y la comunicación con consecuencias apenas imaginables para el futuro de la humanidad.

Para las economías en desarrollo como la nuestra, el maximizar los beneficios que ofrece el comercio electrónico es un imperativo; pero también es lograr una posición de vanguardia en la transferencia de tecnología e información, con base al potencial que tiene nuestro país en cuanto a recursos humanos calificados en el área informática, tecnológica y profesional, en general.

El resultado de este proceso ha sido el advenimiento de la Economía Digital, en la cual el valor recae con mayor fuerza en bienes intangibles, y en el conocimiento. Pero también ha significado una nueva vía amplísima y dinamizadora de comercio.

El desarrollo del comercio electrónico ha sido vertiginoso, sin embargo, presentará obstáculos difíciles de superar si no se resuelven ciertos aspectos técnicos y de índole legal. Desde el punto de vista jurídico esta revolución tecnológica e informática ha significado un reto

legislación procesal civil, es admisible como prueba en sede jurisdiccional.

En concreto, para lograr los objetivos supracitados es preciso: regular el reconocimiento legal expreso de la Firma Digital; determinar los efectos de la Firma Digital; el reconocimiento del principio de equivalencia funcional por medio del cual se confiere al documento digital firmado los mismos efectos que se le imputan al documento escrito; acoger el "principio de neutralidad tecnológica", de forma tal que la normativa no limite el mecanismo de Firma Digital a una sola tecnología: establecer reglas mínimas en materia de conservación, envío y recepción de mensajes de datos para aquellos casos en que las partes no hayan estipulado reglas especiales.

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

DECRETA:

LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES

TÍTULO I

PRINCIPIOS Y NORMAS GENERALES

CAPÍTULO PRIMERO

DISPOSICIONES GENERALES

ARTÍCULO 1.- La presente Ley tiene por objetivo regular el uso y el reconocimiento jurídico de la Firma Digital, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad, así como el autorizar al Estado para su utilización.

ARTÍCULO 2.- Para los propósitos de la presente Ley se establecen las siguientes definiciones:

1.- **Acreditación:** La acreditación es el procedimiento mediante el cual un organismo autorizado reconoce formalmente que una entidad o empresa es competente para realizar tareas específicas.

2.- **Acreditación voluntaria del prestador de servicios de certificación:** Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se emite, a petición del interesado, por el Órgano Rector y la Autoridad Competente de acreditación, de conformidad con lo previsto en esta Ley, su reglamento y la normativa intencional aplicable.

3.- Certificado Digital: Es la certificación digital que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

4.- Certificado Digital Reconocido: Es el certificado que cumple con los requisitos establecidos en la presente Ley y su reglamento, y que vincula un documento digital con determinada persona como su signatario, mediante un proceso seguro de certificación y es expedido por un prestador de servicios de certificación acreditado por el Órgano Rector y la autoridad competente de acreditación.

5.- Datos de creación de firma: Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la Firma Digital.

6.- Datos de verificación de firma: Son los datos como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma Digital.

7.- Dispositivo de creación de firma: Es un mecanismo que sirve para aplicar los datos de creación de firma.

8.- Dispositivo de verificación de firma: Es un mecanismo que sirve para aplicar los datos de verificación de firma.

9.- Dispositivo seguro de creación de firma: Es el mecanismo de creación de firma que cumple adicionalmente con los requisitos establecidos en la presente Ley y su reglamento.

10.- Documento: Significa información que se encuentra almacenada en un medio tangible, o que se guarda en un medio electrónico o de cualquier otra naturaleza, y que se puede recuperar o reproducir en una forma perceptible e inteligible.

11.- Firma Digital: Es el conjunto de datos, anexos a otros datos o datos asociados funcionalmente, utilizados como medio para

identificar formalmente al autor o a los autores del documento que la recoge.

12.- Firma Digital Avanzada: Es la Firma Digital Certificada por un prestador de servicios de certificación debidamente acreditado ante la autoridad competente de acreditación.

13.- Información: Es aquel mensaje comunicado mediante datos, textos, imágenes, sonidos, códigos, programas, información almacenada en bases de datos, aplicaciones, o similares.

14.- Iniciador: Es quien envía un mensaje de datos, esté o no suscrito digitalmente.

15.- Información Íntegra: Se entenderá por íntegra aquella información que haya permanecido completa e inalterada, sin menoscabo de cualquier adición o cambio, inherente al proceso de comunicación, almacenamiento, archivo o presentación. El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.

16.- Intermediario: Es aquella persona, física o jurídica, que actuando por cuenta de otra, envíe, reciba, almacene dicho mensaje o preste algún otro servicio con respecto a él.

17.- Mensaje de datos: Es la información generada, enviada, recibida, almacenada, o comunicada por medios digitales, electrónicos, ópticos o similares.

18.- Prestador de servicios de certificación o entidad certificadora: Es la persona física o jurídica que expide certificados.

19.- Procedimiento seguro: Es el procedimiento empleado con el propósito de verificar que una Firma Digital es atribuible a determinada persona como su signatario, o para detectar cambios y errores en un documento digital, incluyendo cualquier proceso que

implique el uso de algoritmos matemáticos, códigos, sistemas de encriptamiento, y cualquier otro medio o tecnología de identificación o reconocimiento.

20.- Producto de Firma Digital: Es el instrumento y sus componentes específicos, destinados a la prestación de servicios de Firma Digital por el prestador de servicios de certificación o para la creación o verificación de Firma Digital.

21.- Receptor: Es la persona a quien el signatario dirige el mensaje o documento electrónico.

22.- Signatario: Es la persona física o jurídica que cuenta con un mecanismo de creación de firma, que actúa en nombre propio o con poderes de representación de otra persona física o jurídica.

23.- Sistema: Es el conjunto de elementos independientes pero interrelacionados entre sí para conseguir un propósito común.

24.- Sistema de información: Es un conjunto de elementos ordenado utilizado para generar, enviar, recibir, almacenar o procesar de alguna forma mensajes de datos.

ARTÍCULO 3.- En la presente Ley se utilizará el término digital entendido como cualquier información codificada en dígitos, la cual resulta más precisa que el término electrónico, que se refiere al medio físico de procesamiento, almacenamiento o transmisión, el cual es uno de los medios para generar, transmitir y almacenar información digital.

CAPÍTULO II

RECONOCIMIENTO JURÍDICO DE LA FIRMA DIGITAL

ARTÍCULO 4.- La Firma Digital Avanzada, deberá crearse mediante un dispositivo seguro de creación de firma.

ARTÍCULO 5.- La Firma Digital Avanzada, siempre que esté basada en un certificado digital reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma digital, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel.

Cuando la ley exija la presentación o existencia de un documento escrito debidamente firmado, tal requisito será plenamente satisfecho por un documento digital, si el mismo ha sido firmado mediante una Firma Digital Avanzada, creada por un dispositivo seguro de creación de firma.

Se presumirá que la Firma Digital Avanzada y el medio de creación de firma con el que ésta se produzca, reúnen las condiciones necesarias para producir los efectos indicados en este apartado cuando el certificado reconocido es emitido por un prestador de servicios de certificación acreditado.

ARTÍCULO 6.- Cuando una ley requiere que un documento o firma esté certificado o autenticado notarialmente por un abogado, o de cualquier otra forma reconocido, verificado o certificado, tal requisito se tendrá por cumplido si una firma electrónica avanzada de un notario público, abogado, funcionario público, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma digital o Firma Digital avanzada.

CAPÍTULO III

USO DE LA FIRMA DIGITAL Y LOS DOCUMENTOS ELECTRÓNICOS POR EL ESTADO

ARTÍCULO 7.- Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Supremo de Elecciones, Contraloría General de la República, Defensoría de los Habitantes, así como a todas las instituciones públicas descentralizadas, y entes públicos no estatales para la utilización de la Firma Digital avanzada y los documentos electrónicos firmados digitalmente en sus relaciones internas, entre ellos y con los particulares, de conformidad con las previsiones de esta Ley y su reglamento.

TÍTULO II

DE LOS SERVICIOS DE CERTIFICACIÓN DIGITAL

CAPÍTULO I

DEL ÓRGANO RECTOR

ARTÍCULO 8.- El Ministerio de Ciencia y Tecnología será el Órgano Rector en todo lo concerniente a esta Ley.

8.1 Toda interpretación técnica estará bajo el mejor criterio del Órgano Rector tomando en cuenta el estado de arte en la tecnología, así como los requerimientos y realidades del país.

ARTÍCULO 9.- El Poder Ejecutivo, a través del Ministerio de Ciencia y Tecnología, utilizará un sistema de acreditación voluntario, en el ámbito de los prestadores de servicios de certificación de Firma Digital Avanzada, coordinando para ello con la Autoridad de Acreditación, la cual

será un ente con participación activa y equilibrada de los sectores involucrados. La autoridad de acreditación mediante la función de acreditación, reconoce formalmente que una organización es competente para llevar a cabo tareas específicas de acuerdo a los requisitos de normas nacionales e internacionales, que permitan lograr un adecuado grado de seguridad y confianza que proteja debidamente, los derechos de los usuarios, para lo cual deberá llevar a cabo el proceso de evaluación correspondiente, un registro de las entidades acreditadas y velar por que se cumplan los requisitos establecidos por esta Ley y su reglamento.

CAPÍTULO II

CERTIFICADOS DIGITALES

ARTÍCULO 10.- Los certificados digitales se vinculan con una persona confirmando su identidad, los cuales deberán contener al menos:

1.- Los datos que identifiquen individualmente al firmante.

2.- Los datos que identifiquen a la entidad de certificación.

3.- Número de serie del certificado.

4.- Fecha de emisión y plazo de vigencia.

5.- Los demás que el reglamento establezca.

ARTÍCULO 11.- Los certificados digitales se podrán cancelar y revocar en los siguientes casos:

1.- A solicitud del titular de la firma.

2.- Por expiración del plazo.

3.- Por cese de operaciones de la entidad de certificación.

4.- Por muerte del titular de la Firma Digital.

5.- Por incumplimiento contractual con la entidad de certificación.

6.- Las demás que el reglamento establezca.

ARTÍCULO 12.- Los certificados de Firma Digital que sean emitidos por entidades no establecidas en Costa Rica, serán equivalentes a los otorgados por prestadores establecidos en el país, cuando hayan sido homologados por estos últimos, bajo su responsabilidad, y reconocidos por la autoridad de acreditación competente y cumpliendo con los requisitos fijados en esta Ley, su reglamento y normas internacionales correspondientes.

CAPÍTULO III

DE LA ACREDITACIÓN E INSPECCIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DIGITAL

ARTÍCULO 13.- Mediante la autoridad competente de acreditación, la cual estará adscrita al Ministerio Rector, las empresas que emitan certificados de Firma Digital, deberán someterse al proceso de acreditación que se defina al respecto para estar debidamente acreditados. Las funciones de las empresas certificadoras serán entre otras las de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado.

ARTÍCULO 14.- Con el fin de comprobar el cumplimiento de las obligaciones de los prestadores acreditados, la Autoridad de Acreditación ejercerá la facultad de inspección sobre los prestadores acreditados y podrá, a tal efecto, requerir información, ordenar evaluaciones anunciadas o no anunciadas a sus instalaciones al menos una vez al año y solicitar las modificaciones necesarias para que se mantenga actualizado el sistema y el servicio, con personal que para tal efecto se seleccione de conformidad al reglamento, la Autoridad de Acreditación y del Órgano Rector. Así como suspender las acreditaciones en caso de incumplimiento.

ARTÍCULO 15.- La Autoridad de Acreditación así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen las empresas certificadoras.

ARTÍCULO 16.- El Órgano Rector deberá observar en sus actuaciones y regulaciones total neutralidad respecto de las diversas tecnologías de Firma Digital existentes, procurando la mayor adaptabilidad a los avances científicos y tecnológicos en tal área.

TÍTULO III

LOS DISPOSITIVOS DE FIRMA DIGITAL AVANZADA Y LA EVALUACIÓN DE SU CONFORMIDAD CON LA NORMATIVA APLICABLE

CAPÍTULO ÚNICO

ARTÍCULO 17.- Los dispositivos seguros de creación de Firma Digital para considerarse como tales deberán cumplir con:

1.- Garantizar que los datos utilizados para la generación de firma puedan producirse sólo una vez y asegurar, razonablemente, su secreto, dentro de las posibilidades o limitaciones tecnológicas.

2.- Que exista seguridad razonable de que dichos datos no puedan ser alterados o falsificados con la tecnología existente en un momento dado.

3.- Que los datos de creación de firma puedan ser protegidos con fiabilidad por el signatario contra la utilización por otros.

4.- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma.

ARTÍCULO 18.- Los dispositivos de verificación de Firma Digital Avanzada deben garantizar al menos lo siguiente:

1.- Que la firma se verifique de forma fiable y el resultado de la verificación figure correctamente.

2.- Que el verificador pueda, en caso necesario, establecer de forma fiable la integridad de los datos firmados y detectar si han sido modificados.

3.- Que aparezca correctamente la identidad del signatario.

4.- Que se verifique de forma fiable el certificado.

5.- Que pueda detectarse cualquier cambio relativo a su seguridad e integridad.

ARTÍCULO 19.- Las disposiciones de esta Ley no deberán entenderse en el sentido de prohibir la existencia de sistemas de Firma Digital basados en convenios expresos entre las partes, las que podrán a través de un contrato fijar sus derechos y obligaciones, y las condiciones técnicas y de cualquier otra clase, bajo las cuales reconocerán su autoría sobre un documento digital o mensaje de datos que envíen, o la recepción de un mensaje de datos de su contraparte.

TÍTULO IV

DISPOSICIONES FINALES

ARTÍCULO 20.- El Poder Ejecutivo deberá emitir el reglamento a la presente Ley dentro del plazo máximo de tres meses siguientes a su publicación.

Rige a partir de su publicación.

Miguel Ángel Rodríguez Echeverría

PRESIDENTE DE LA REPÚBLICA

Guy de Téramond
MINISTRO DE CIENCIA
Y TECNOLOGÍA

22 de febrero de 2001, gdph.

NOTA: Este proyecto pasó a estudio e informe de la Comisión Especial de Propiedad Intelectual.

DIRECTIVA 1999/93/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 13 de diciembre de 1999

por la que se establece un marco comunitario para la firma electrónica

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, el apartado 2 de su artículo 47 y sus artículos 55 y 95,

Vista la propuesta de la Comisión [1],

Visto el dictamen del Comité Económico y Social [2],

Visto el dictamen del Comité de las Regiones [3],

De conformidad con el procedimiento establecido en el artículo 251 del Tratado [4],

Considerando lo siguiente:

(1) El 16 de abril de 1997, la Comisión presentó al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones la comunicación «Iniciativa europea de comercio electrónico».

(2) El 8 de octubre de 1997, la Comisión presentó al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones la comunicación «El Fomento de la seguridad y la confianza en la comunicación electrónica: hacia un marco europeo para la firma digital y el cifrado».

(3) El 1 de diciembre de 1997, el Consejo invitó a la Comisión a que presentara lo antes posible una propuesta de directiva del Parlamento Europeo y del Consejo sobre la firma digital.

(4) La comunicación y el comercio electrónicos requieren firmas electrónicas y servicios conexos de autenticación de datos. La heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y acreditación de los proveedores de servicios de certificación entre los Estados miembros puede entorpecer gravemente el uso de las comunicaciones electrónicas y el comercio electrónico. Por otro lado, un marco claro comunitario sobre las condiciones aplicables a la firma electrónica aumentará la confianza en las nuevas tecnologías y la aceptación general de las mismas. La legislación de los Estados miembros en este ámbito no debería obstaculizar la libre circulación de bienes y servicios en el mercado interior.

(5) Es preciso promover la interoperabilidad de los productos de firma electrónica; de conformidad con el artículo 14 del Tratado, el mercado interior implica un espacio sin fronteras interiores en el que está garantizada la libre circulación de mercancías. Deben satisfacerse los requisitos esenciales específicos de los productos de firma electrónica a fin de garantizar la libre circulación en el mercado interior y fomentar la confianza en la firma electrónica, sin perjuicio de lo dispuesto en el Reglamento (CE) nº 3381/94 del Consejo, de 19 de diciembre de 1994, por el que se establece un régimen comunitario de control de las exportaciones de productos de doble uso [5] y en la Decisión 94/942/PESC del Consejo, de 19 de diciembre de 1994, relativa a la Acción común adoptada por el Consejo referente al control de las exportaciones de productos de doble uso [6].

(6) La presente Directiva no armoniza la prestación de servicios por lo que respecta a la confidencialidad de la información cuando sean objeto de disposiciones nacionales en materia de orden público y seguridad pública.

(7) El mercado interior garantiza también la libre circulación de personas, por lo cual es cada vez más frecuente que los ciudadanos y residentes de la Unión Europea tengan que tratar con autoridades de Estados miembros distintos de aquél en el que residen. La disponibilidad de la comunicación electrónica puede ser de gran utilidad a este respecto.

(8) Los rápidos avances tecnológicos y la dimensión mundial de Internet hacen necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos.

(9) La firma electrónica se utilizará en muy diversas circunstancias y aplicaciones, dando lugar a una gran variedad de nuevos servicios y productos relacionados con ella o que la utilicen. La definición de dichos productos y servicios no debe limitarse a la expedición y gestión de certificados, sino incluir también cualesquiera otros servicios o productos que utilicen firmas electrónicas o se sirvan de ellas, como los servicios de registro, los servicios de estampación de fecha y hora, los servicios de guías de usuarios, los de cálculo o asesoría relacionados con la firma electrónica.

(10) El mercado interior permite a los proveedores de servicios de certificación llevar a cabo sus actividades transfronterizas para acrecentar su competitividad y, de ese modo, ofrecer a los consumidores y a las empresas nuevas posibilidades de intercambiar información y comerciar electrónicamente de una forma segura, con independencia de las fronteras. Con objeto de estimular la prestación de servicios de certificación en toda la Comunidad a través de redes abiertas, los proveedores de servicios de certificación deben tener libertad para prestar sus servicios sin autorización previa. La autorización previa implica no sólo el permiso que ha de

---

[1] DO C 325 de 23.10.1998, p. 5.
[2] DO C 40 de 15.2.1999, p. 29.
[3] DO C 93 de 6.4.1999, p. 33.
[4] Dictamen del Parlamento Europeo de 13 de enero de 1999 (DO C 104 de 14.4.1999, p. 49), Posición común del Consejo de 28 de junio de 1999 (DO C 243 de 27.8.1999, p. 83) y Decisión del Parlamento Europeo de 27 de octubre de 1999 (no publicada aún en el Diario Oficial), Decisión del Consejo de 30 de noviembre de 1999.
[5] DO L 367 de 31.12.1994, p. 1; Reglamento modificado por el Reglamento (CE) nº 837/95 (DO L 90 de 21.4.1995, p. 1).
[6] DO L 367 de 31.12.1994, p. 8; Decisión cuya última modificación la constituye la Decisión 1999/193/CE (DO L 73 de 19.3.1999, p. 1).

obtener el proveedor de servicios de certificación interesado en virtud de una decisión de las autoridades nacionales antes de que se le permita prestar sus servicios de certificación, sino también cualesquiera otras medidas que tengan ese mismo efecto.

(11) Los sistemas voluntarios de acreditación destinados a un nivel reforzado de prestación de servicios pueden aportar a los proveedores de servicios de certificación un marco apropiado para aproximarse a los niveles de confianza, seguridad y calidad exigidos por un mercado en evolución. Dichos sistemas deben fomentar la adopción de las mejores prácticas por parte de los proveedores de servicios de certificación; debe darse a los proveedores de servicios de certificación libertad para adherirse a dichos sistemas de acreditación y disfrutar de sus ventajas.

(12) Los servicios de certificación pueden ser prestados tanto por entidades públicas como por personas físicas o jurídicas cuando así se establezca de acuerdo con el Derecho nacional. Los Estados miembros no deben prohibir a los proveedores de servicios de certificación operar al margen de los sistemas de acreditación voluntaria; ha de velarse por que los sistemas de acreditación no supongan mengua de la competencia en el ámbito de los servicios de certificación.

(13) Los Estados miembros pueden decidir cómo llevar a cabo la supervisión del cumplimiento de lo dispuesto en la presente Directiva. La presente Directiva no excluye el establecimiento de sistemas de supervisión basados en el sector privado. La presente Directiva no obliga a los proveedores de servicios de certificación a solicitar ser supervisados con arreglo a cualquier sistema de acreditación aplicable.

(14) Es importante alcanzar un equilibrio entre las necesidades de los consumidores y las de las empresas.

(15) El anexo III abarca los requisitos de los dispositivos seguros de creación de firmas electrónicas para garantizar la funcionalidad de las firmas electrónicas avanzadas; no abarca la totalidad del sistema en cuyo entorno operan dichos dispositivos. El funcionamiento del mercado interior exige que la Comisión y los Estados miembros actúen con celeridad para hacer posible la designación de los organismos encargados de evaluar la conformidad de los dispositivos seguros de firma con el anexo III. Con objeto de subvenir a las necesidades del mercado, la evaluación de la conformidad ha de producirse oportunamente y ser eficaz.

(16) La presente Directiva contribuye al uso y al reconocimiento legal de la firma electrónica en la Comunidad; no se precisa un marco reglamentario para las firmas electrónicas utilizadas exclusivamente dentro de sistemas basados en acuerdos voluntarios de Derecho privado celebrados entre un número determinado de participantes. En la medida en que lo permita la legislación nacional, ha de respetarse la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas; no se debe privar a las firmas electrónicas utilizadas en estos sistemas de eficacia jurídica ni de su carácter de prueba en los procedimientos judiciales.

(17) La presente Directiva no pretende armonizar las legislaciones nacionales sobre contratos, en particular por lo que respecta al perfeccionamiento y eficacia de los mismos, ni tampoco otras formalidades de naturaleza no contractual relativas a la firma; por dicho motivo, las disposiciones sobre los efectos legales de la firma electrónica deberán entenderse sin perjuicio de los requisitos de forma establecidos por las legislaciones nacionales en materia de celebración de contratos, ni para las normas que determinan el lugar en que se considera celebrado un contrato.

(18) El almacenamiento y la copia de los datos de creación de la firma pueden poner en peligro la validez jurídica de la firma electrónica.

(19) La firma electrónica se utilizará en el sector público en el marco de las administraciones nacionales y comunitaria y en la comunicación entre dichas administraciones y entre éstas y los ciudadanos y agentes económicos, por ejemplo en la contratación pública, la fiscalidad, la seguridad social, la atención sanitaria y el sistema judicial.

(20) Unos criterios armonizados en relación con la eficacia jurídica de la firma electrónica mantendrán un marco jurídico coherente en toda la Comunidad. Las legislaciones nacionales establecen requisitos divergentes con respecto a la validez jurídica de las firmas manuscritas; se pueden utilizar certificados para confirmar la identidad de la persona que firma electrónicamente; las firmas electrónicas avanzadas basadas en un certificado reconocido pretenden lograr un mayor nivel de seguridad. Las firmas electrónicas avanzadas relacionadas con un certificado reconocido y creadas mediante un dispositivo seguro de creación de firma únicamente pueden considerarse jurídicamente equivalentes a las firmas manuscritas si se cumplen los requisitos aplicables a las firmas manuscritas.

(21) Para contribuir a la aceptación general de los métodos de autenticación electrónica, debe garantizarse la admisibilidad de la firma electrónica como prueba en procedimientos judiciales en todos los Estados miembros. El reconocimiento legal de la firma electrónica debe basarse en criterios objetivos y no estar supeditado a la autorización del proveedor de servicios de certificación de que se trate; la legislación nacional rige la determinación de los ámbitos jurídicos en los que pueden usarse los documentos electrónicos y de la firma electrónica. La presente Directiva se entiende sin perjuicio de la facultad de los tribunales nacionales para dictar resoluciones acerca de la conformidad con los requisitos de la presente Directiva y no afecta a las normas nacionales en lo que se refiere a la libertad de la valoración judicial de las pruebas.

(22) Los proveedores de servicios de certificación al público están sujetos a la normativa nacional en materia de responsabilidad.

(23) El desarrollo del comercio electrónico internacional requiere acuerdos transfronterizos que implican a terceros países; para garantizar la interoperabilidad a nivel mundial, podría ser beneficioso celebrar acuerdos con terceros países sobre normas multilaterales en materia de reconocimiento mutuo de servicios de certificación.

(24) Para incrementar la confianza de los usuarios en la comunicación y el comercio electrónicos, los proveedores de servicios de certificación deben observar la normativa sobre protección de datos y el respeto de la intimidad.

(25) Las disposiciones relativas al uso de seudónimos en los certificados no deben impedir a los Estados miembros exigir la identificación de las personas de conformidad con el Derecho comunitario o nacional.

(26) Habida cuenta de que las medidas necesarias para la ejecución de la presente Directiva son medidas de gestión con arreglo al artículo 2 de la Decisión 1999/468/CE del Consejo, de 28 de junio de 1999, por la que se establecen los procedimientos para el ejercicio de las competencias de ejecución atribuidas a la Comisión [1], dichas medidas deben ser aprobadas con arreglo al procedimiento de gestión previsto en el artículo 4 de la citada Decisión.

(27) Transcurridos dos años desde su aplicación, la Comisión procederá a una revisión de la presente Directiva a fin de cerciorarse de que los avances tecnológicos y los cambios del entorno jurídico no han creado obstáculos al logro de los objetivos formulados en la presente Directiva. La Comisión debe estudiar la incidencia de ámbitos técnicos afines y presentar un informe al respecto al Parlamento Europeo y al Consejo.

(28) De conformidad con los principios de subsidiariedad y proporcionalidad recogidos en el artículo 5 del Tratado, el objetivo de crear un marco jurídico armonizado para la prestación del servicio de firma electrónica y de servicios conexos no puede ser alcanzado de manera suficiente por los Estados miembros y, por consiguiente, puede lograrse mejor a nivel comunitario. La presente Directiva no excede de lo necesario para lograr dicho objetivo,

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Ámbito de aplicación

La presente Directiva tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico. La presente Directiva crea un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior.

La presente Directiva no regula otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectan a las normas y límites, contenidos en las legislaciones nacionales o comunitaria, que rigen el uso de documentos.

Artículo 2

Definiciones

A efectos de la presente Directiva, se entenderá por:

1) «firma electrónica»: los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación;

2) «firma electrónica avanzada»: la firma electrónica que cumple los requisitos siguientes:

   a) estar vinculada al firmante de manera única;

   b) permitir la identificación del firmante;

   c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;

   d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable;

3) «firmante»: la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa;

4) «datos de creación de firma»: los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica;

5) «dispositivo de creación de firma»: un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma;

6) «dispositivo seguro de creación de firma»: un dispositivo de creación de firma que cumple los requisitos enumerados en el anexo III;

7) «datos de verificación de firma»: los datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica;

8) «dispositivo de verificación de firma»: un programa informático configurado o un aparato informático configurado, que sirve para aplicar los datos de verificación de firma;

9) «certificado»: la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta;

10) «certificado reconocido»: el certificado que cumple los requisitos establecidos en el anexo I y es suministrado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el anexo II;

11) «proveedor de servicios de certificación»: la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica;

12) «producto de firma electrónica»: el programa informático o el material informático, o sus componentes específicos, que se destinan a ser utilizados por el proveedor de servicios de certificación para la prestación de servicios de firma electrónica o que se destinan a ser utilizados para la creación o la verificación de firmas electrónicas;

13) «acreditación voluntaria»: todo permiso que establezca derechos y obligaciones específicas para la prestación de servicios de certificación, que se concedería, a petición del proveedor de servicios de certificación interesado, por el organismo público o privado encargado del establecimiento y supervisión del cumplimiento de dichos derechos y obligaciones, cuando el proveedor de servicios de certificación no esté habilitado para ejercer los derechos derivados del permiso hasta que haya recaído la decisión positiva de dicho organismo.

[1] DO L 184 de 17.7.1999, p. 23.

Artículo 3

Acceso al mercado

1. Los Estados miembros no condicionarán la prestación de servicios de certificación a la obtención de autorización previa.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán establecer o mantener sistemas voluntarios de acreditación destinados a mejorar los niveles de provisión de servicios de certificación. Todas las condiciones relativas a tales sistemas deberán ser objetivas, transparentes, proporcionadas y no discriminatorias. Los Estados miembros no podrán limitar el número de proveedores de servicios de certificación acreditados amparándose en la presente Directiva.

3. Los Estados miembros velarán por que se establezca un sistema adecuado que permita la supervisión de los proveedores de servicios de certificación establecidos en su territorio que expiden al público certificados reconocidos.

4. La conformidad de los dispositivos seguros de creación de firma con los requisitos fijados en el anexo III será determinada por los organismos públicos o privados pertinentes, designados por los Estados miembros. La Comisión, con arreglo al procedimiento del artículo 9, establecerá criterios para que los Estados miembros determinen si procede designar un determinado organismo.

La conformidad con los requisitos del anexo III establecida por dichos organismos será reconocida por todos los Estados miembros.

5. La Comisión, con arreglo al procedimiento del artículo 9, podrá determinar, y publicar en el *Diario Oficial de las Comunidades Europeas*, los números de referencia de las normas que gocen de reconocimiento general para productos de firma electrónica. Los Estados miembros presumirán que los productos de firma electrónica que se ajusten a dichas normas son conformes con lo prescrito en la letra f) del anexo II y en el anexo III de la presente Directiva.

6. Los Estados miembros y la Comisión cooperarán para promover el desarrollo y la utilización de los dispositivos de creación de firma, a la luz de las recomendaciones para la verificación segura de firma que figuran en el anexo IV y en interés del consumidor.

7. Los Estados miembros podrán supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales. Tales prescripciones serán objetivas, transparentes, proporcionadas y no discriminatorias, y sólo podrán hacer referencia a las características específicas de la aplicación de que se trate. Estas prescripciones no deberán obstaculizar los servicios transfronterizos al ciudadano.

Artículo 4

Principios del mercado interior

1. Los Estados miembros aplicarán las disposiciones nacionales que adopten en cumplimiento de la presente Directiva a los proveedores de servicios de certificación establecidos en su territorio y a los servicios prestados por ellos. Los Estados miembros no podrán restringir la prestación de servicios de certificación en los ámbitos regulados por la presente Directiva que procedan de otro Estado miembro.

2. Los Estados miembros velarán por que los productos de firma electrónica que se ajusten a lo dispuesto en la presente Directiva puedan circular libremente en el mercado interior.

Artículo 5

Efectos jurídicos de la firma electrónica

1. Los Estados miembros procurarán que la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma:

a) satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel; y

b) sea admisible como prueba en procedimientos judiciales.

2. Los Estados miembros velarán por que no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho de que:

— ésta se presente en forma electrónica, o

— no se base en un certificado reconocido, o

— no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o

— no esté creada por un dispositivo seguro de creación de firma.

Artículo 6

Responsabilidad

1. Los Estados miembros garantizarán, como mínimo, que el proveedor de servicios de certificación que expida al público un certificado presentado como certificado reconocido o que garantice al público tal certificado, será responsable por el perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en el certificado por lo que respecta a:

a) la veracidad, en el momento de su expedición, de toda la información contenida en el certificado reconocido y la inclusión en el certificado de toda la información prescrita para los certificados reconocidos;

b) la garantía de que, en el momento de la expedición del certificado, obraban en poder del firmante identificado en el certificado reconocido los datos de creación de firma correspondientes a los datos de verificación de firma que constan o se identifican en el certificado;

c) la garantía de que los datos de creación y de verificación de firma pueden utilizarse complementariamente, en caso de que el proveedor de servicios de certificación genere ambos;

salvo que el proveedor de servicios de certificación demuestre que no ha actuado con negligencia.

2. Los Estados miembros garantizarán como mínimo que el proveedor de servicios de certificación que haya expedido al público un certificado presentado como certificado reconocido será responsable por el perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en dicho certificado por no haber registrado la revocación del certificado, salvo que el proveedor de servicios de certificación pruebe que no ha actuado con negligencia.

3. Los Estados miembros velarán por que el proveedor de servicios de certificación pueda consignar en un certificado reconocido límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles para terceros. El proveedor de servicios de certificación no deberá responder de los daños y perjuicios causados por el uso de un certificado reconocido que exceda de los límites indicados en el mismo.

4. Los Estados miembros velarán por que el proveedor de servicios de certificación pueda consignar en el certificado reconocido un valor límite de las transacciones que puedan realizarse con el mismo, siempre y cuando los límites sean reconocibles para terceros.

El proveedor de servicios de certificación no será responsable por los perjuicios que pudieran derivarse de la superación de este límite máximo.

5. Las disposiciones de los apartados 1 a 4 se aplicarán sin perjuicio de la Directiva 93/13/CEE, del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores [1].

Artículo 7

Aspectos internacionales

1. Los Estados miembros velarán por que los certificados expedidos al público como certificados reconocidos por un proveedor de servicios de certificación establecido en un tercer país, sean reconocidos como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad si se cumple alguna de las condiciones siguientes:

a) que el proveedor de servicios de certificación cumpla los requisitos establecidos en la presente Directiva y haya sido acreditado en el marco de un sistema voluntario de acreditación establecido en un Estado miembro;

b) que un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones de la presente Directiva, avale el certificado;

c) que el certificado o el proveedor de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

2. Para facilitar tanto la prestación de servicios transfronterizos de certificación con terceros países como el reconocimiento legal de las firmas electrónicas avanzadas originarias de estos últimos, la Comisión presentará, en su caso, propuestas para lograr el efectivo establecimiento de normas y acuerdos internacionales aplicables a los servicios de certificación. En particular, y en caso necesario, solicitará al Consejo mandatos para la negociación de acuerdos bilaterales y multilaterales con terceros países y organizaciones internacionales. El Consejo se pronunciará por mayoría cualificada.

3. Cuando la Comisión sea informada de cualquier dificultad encontrada por las empresas comunitarias en relación con el acceso al mercado en terceros países, podrá, en caso necesario, presentar propuestas al Consejo para obtener un mandato adecuado para la negociación de derechos comparables para las empresas comunitarias en dichos terceros países. El Consejo se pronunciará por mayoría cualificada.

Las medidas tomadas en virtud del presente apartado se entenderán sin perjuicio de las obligaciones de la Comunidad y de los Estados miembros con arreglo a los acuerdos internacionales pertinentes.

Artículo 8

Protección de datos

1. Los Estados miembros velarán por que los proveedores de servicios de certificación y los organismos nacionales competentes en materia de acreditación y supervisión cumplan los requisitos establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [2].

2. Los Estados miembros velarán por que los proveedores de servicios de certificación que expidan al público certificados únicamente puedan recabar datos personales directamente del titular de los datos o previo consentimiento explícito de éste, y sólo en la medida necesaria para la expedición y el mantenimiento del certificado. Los datos no podrán obtenerse o tratarse con fines distintos sin el consentimiento explícito de su titular.

3. Sin perjuicio de los efectos jurídicos concedidos a los seudónimos con arreglo al Derecho nacional, los Estados miembros no impedirán al proveedor de servicios de certificación que consigne en el certificado un seudónimo del firmante en lugar de su verdadero nombre.

Artículo 9

Comité

1. La Comisión estará asistida por el Comité de firma electrónica (denominado en lo sucesivo «el Comité»), compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

2. En los casos en que se haga referencia al presente apartado, se aplicará el procedimiento de gestión previsto en el artículo 4 de la Decisión 1999/468/CE observando lo dispuesto en el artículo 8 de la misma.

El plazo previsto en el apartado 3 del artículo 4 de la Decisión 1999/468/CE será de tres meses.

3. El Comité aprobará su Reglamento interno.

Artículo 10

Funciones del Comité

El Comité procederá a la clarificación de los requisitos establecidos en los anexos, los criterios a que se refiere el apartado 4 del artículo 3 y las normas para los productos de firma electrónica que gocen de reconocimiento general establecidas y publicadas con arreglo a lo dispuesto en el apartado 5 del artículo 3, conforme al procedimiento establecido en el apartado 2 del artículo 9.

[1] DO L 95 de 21.4.1993, p. 29.

[2] DO L 281 de 23.11.1995, p. 31.

ANEXO I

Requisitos de los certificados reconocidos

Los certificados reconocidos habrán de contener:

a) la indicación de que el certificado se expide como certificado reconocido;

b) la identificación del proveedor de servicios de certificación y el Estado en que está establecido;

c) el nombre y los apellidos del firmante o un seudónimo que conste como tal;

d) un atributo específico del firmante, en caso de que fuera significativo en función de la finalidad del certificado;

e) los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del firmante;

f) una indicación relativa al comienzo y fin del período de validez del certificado;

g) el código indentificativo del certificado;

h) la firma electrónica avanzada del proveedor de servicios de certificación que expide el certificado;

i) los límites de uso del certificado, si procede; y

j) los límites del valor de las transacciones para las que puede utilizarse el certificado, si procede.

ANEXO II

Requisitos de los proveedores de servicios de certificación que expiden certificados ~~reconocidos~~

Los proveedores de servicios de certificación deberán:

a) demostrar la fiabilidad necesaria para prestar servicios de certificación;

b) garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato;

c) garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado;

d) comprobar debidamente, de conformidad con el Derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido;

e) emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados, en particular: competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados; deben poner asimismo en práctica los procedimientos administrativos y de gestión adecuados y conformes a normas reconocidas;

f) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan;

g) tomar medidas contra la falsificación de certificados y, en caso de que el proveedor de servicios de certificación genere datos de creación de firma, garantizar la confidencialidad durante el proceso de generación de dichos datos;

h) disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Directiva, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, por ejemplo contratando un seguro apropiado;

i) registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos;

j) no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves;

k) antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, pudiendo transmitirse electrónicamente, y deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de dicha información estarán también disponibles a instancias de terceros afectados por el certificado;

l) utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:

— sólo personas autorizadas puedan hacer anotaciones y modificaciones,

— pueda comprobarse la autenticidad de la información,

— los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado, y

— el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados.

ANEXO III

Requisitos de los dispositivos seguros de creación de firma electrónica

1. Los dispositivos seguros de creación de firma garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:

   a) los datos utilizados para la generación de firma sólo pueden producirse una vez en la práctica y se garantiza razonablemente su secreto;

   b) existe la seguridad razonable de que los datos utilizados para la generación de firma no pueden ser hallados por deducción y la firma está protegida contra la falsificación mediante la tecnología existente en la actualidad;

   c) los datos utilizados para la generación de firma pueden ser protegidos de forma fiable por el firmante legítimo contra su utilización por otros.

2. Los dispositivos seguros de creación de firma no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes del proceso de firma.

ANEXO IV

Recomendaciones para la verificación segura de firma

Durante el proceso de verificación de firma, deberá garantizarse, con suficiente certeza, que:

a) los datos utilizados para verificar la firma corresponden a los datos mostrados al verificador;

b) la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente;

c) el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados;

d) se verifican de forma fiable la autenticidad y la validez del certificado exigido al verificarse la firma;

e) figuran correctamente el resultado de la verificación y la identidad del firmante;

f) consta claramente la utilización de un seudónimo; y

g) puede detectarse cualquier cambio pertinente relativo a la seguridad.

La firma electrónica ya tiene eficacia jurídica

La Administración española ha dado luz verde al texto que regula los aspectos jurídicos relativos a la firma electrónica, dándole la misma validez que a la firma manuscrita. La nueva norma se publica al abrigo de la posición común número 28/1999 (1999/C 243/02) de la Unión Europea. En España existen empresas con suficiente capacidad tecnológica que pueden prestar servicios de certificación con suficiente seguridad jurídica.

Real Decreto Ley 14/1999,

de 17 de septiembre, sobre firma electrónica

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

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

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

Por ello, este Real Decreto-ley persigue, respetando el contenido de la posición común respecto de la Directiva sobre firma electrónica, establecer una regulación clara del uso de ésta, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación. De igual modo, este Real Decreto ley determina el registro en el que habrán de inscribirse los prestadores de servicios de certificación y el régimen de inspección administrativa de su actividad, regula la expedición y la pérdida de eficacia de los certificados y tipifica las infracciones y las sanciones que se prevén para garantizar su cumplimiento.

La presente disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio de 1998, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio.

En su virtud, a propuesta del Ministro de Fomento, de la Ministra de Justicia y del Ministro de Industria y Energía, previo informe del Consejo General del Poder Judicial y de la Agencia de Protección de Datos, tras la deliberación del Consejo de Ministros, en su reunión celebrada el día 17 de septiembre de 1999, y en uso de la autorización concedida en el artículo 86 de la Constitución,

DISPONGO:

TITULO PRIMERO

Disposiciones generales

CAPITULO UNICO

Artículo 1. Ambito de aplicación.

1. Este Real Decreto-ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

2. Las disposiciones contenidas en este Real Decreto-ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones.

Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

Artículo 2. Definiciones.

A los efectos de este Real Decreto-ley, se establecen las siguientes definiciones:

a) "Firma electrónica": Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

b) "Firma electrónica avanzada": Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

c) "Signatario": Es la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

d) "Datos de creación de firma": Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica.

e) "Dispositivo de creación de firma": Es un programa o un aparato informático que sirve para aplicar los datos de creación de firma.

f) "Dispositivo seguro de creación de firma": Es un dispositivo de creación de firma que cumple los requisitos establecidos en el artículo 19.

g) "Datos de verificación de firma": Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

h) "Dispositivo de verificación de firma": Es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma.

i) "Certificado": Es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

j) "Certificado reconocido": Es el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12.

k) "Prestador de servicios de certificación": Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

l) "Producto de firma electrónica": Es un programa o un aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

ll) "Acreditación voluntaria del prestador de servicios de certificación": Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

Artículo 3. Efectos jurídicos de la firma electrónica.

1. La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21.

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

TITULO II

La prestación de servicios de certificación

CAPITULO PRIMERO

Principios generales

Artículo 4. Régimen de libre competencia.

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realiza en régimen de libre competencia, sin que quepa establecer restricciones para los servicios de certificación que procedan de alguno de los Estados miembros de la Unión Europea.

2. La prestación de los servicios de certificación por las Administraciones o los organismos o sociedades de ellas dependientes se realizará con la debida separación de cuentas y con arreglo a los principios de objetividad, transparencia y no discriminación.

Artículo 5. Empleo de la firma electrónica por las Administraciones públicas.

1. Se podrá supeditar por la normativa estatal o, en su caso, autonómica el uso de la firma electrónica en el seno de las Administraciones públicas y sus entes públicos y en las relaciones que con cualesquiera de ellos mantengan los particulares, a las condiciones adicionales que se consideren necesarias, para salvaguardar las garantías de cada procedimiento.

Las condiciones adicionales que se establezcan podrán incluir la prestación de un servicio de consignación de fecha y hora, respecto de los documentos electrónicos integrados en un expediente administrativo. El citado servicio consistirá en la acreditación por el prestador de servicios de certificación, o por un tercero, de la fecha y hora en que un documento electrónico es enviado por el signatario o recibido por el destinatario.

Las normas estatales que regulen las condiciones adicionales sobre el uso de la firma electrónica a las que se refiere este apartado sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y se dictarán a propuesta del Ministerio de Administraciones Públicas y previo informe del Consejo Superior de Informática.

2. Las condiciones adicionales a las que se refiere el apartado anterior deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, serán objetivas, razonables y no discriminatorias y no obstaculizarán la prestación de servicios al ciudadano, cuando en ella intervengan distintas Administraciones públicas nacionales o extranjeras.

3. Podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa. Asimismo, el Ministro de Economía y Hacienda, respetando las condiciones previstas en este Real Decreto-ley, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarias, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica.

Artículo 6. Sistemas de acreditación de prestadores de servicios de certificación y de certificación de productos de firma electrónica.

1. El Gobierno, por Real Decreto, podrá establecer sistemas voluntarios de acreditación de los prestadores de servicios de certificación de firma electrónica, determinando, para ello, un régimen que permita lograr el adecuado grado de seguridad y proteger, debidamente, los derechos de los usuarios.

2. Las funciones de certificación a las que se refiere este Real Decreto-ley serán ejercidas por los órganos, en cada caso competentes, referidos en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones; en la Ley 21/1992, de 16 de julio, de Industria, y en la

demás legislación vigente sobre la materia. El Real Decreto al que se refiere el apartado 1 establecerá las condiciones que permitan coordinar los sistemas de certificación.

3. Las normas que regulen los sistemas de acreditación y de certificación deberán ser objetivas, razonables y no discriminatorias. Todos los prestadores de servicios que se sometan voluntariamente a ellos, podrán obtener la correspondiente acreditación de su actividad o, en su caso, la certificación del producto de firma electrónica que empleen.

4. Los órganos competentes para el ejercicio de las funciones a que se refiere el apartado anterior valorarán los informes técnicos que emitan las entidades de evaluación sobre los prestadores de servicios que hayan solicitado su acreditación o los productos para los que se haya pedido certificación. También tomarán en cuenta el cumplimiento, por el prestador de servicios, de los requisitos que se determinen reglamentariamente para poder ser acreditado.

5. A los efectos de este Real Decreto-ley, sólo podrán actuar como entidades de evaluación aquellas que hayan sido acreditadas por el organismo independiente al que se haya atribuido esta facultad por el Real Decreto al que se refiere el apartado primero de este artículo.

Artículo 7. Registro de Prestadores de Servicios de Certificación.

1. Se crea, en el Ministerio de Justicia, el Registro de Prestadores de Servicios de Certificación, en el que deberán solicitar su inscripción, con carácter previo al inicio de su actividad, todos los establecidos en España. Su regulación se desarrollará por Real Decreto.

2. La solicitud de inscripción habrá de formularse, aportando la documentación que se establezca reglamentariamente, a efectos de la identificación del prestador de servicios de certificación y de justificar que éste reúne los requisitos necesarios, en cada caso, para ejercer su actividad. También será objeto de inscripción ulterior cualquier circunstancia relevante, a efectos de este Real Decreto-ley, relativa al prestador de servicios de certificación, como su acreditación o estar en condiciones de expedir certificados reconocidos.

La formulación de la solicitud de inscripción en el Registro por los citados prestadores de servicios, les permitirá iniciar o continuar su actividad, sin perjuicio de la aplicación, en su caso, del régimen sancionador correspondiente.

3. El Registro de Prestadores de Servicios de Certificación será público y deberá mantener permanentemente actualizada y a disposición de cualquier persona una relación de los inscritos, en la que figurarán su nombre o razón social, la dirección de su página en Internet o de correo electrónico, los datos de verificación de su firma electrónica y, en su caso, su condición de acreditado o de tener la posibilidad de expedir certificados reconocidos. En la citada relación figurarán, también, cualesquiera otros datos complementarios que se determinen por Real Decreto.

Los datos inscritos en el Registro podrán ser consultados por vía telemática o a través de la oportuna certificación registral. El suministro de esta información podrá sujetarse al pago de una tasa, cuyos elementos esenciales se determinarán por ley.

CAPITULO II

Certificados

Artículo 8. Requisitos para la existencia de un certificado reconocido.

1. Los certificados reconocidos, definidos en el artículo 2 j) de este Real Decreto-ley, tendrán el siguiente contenido:

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.

f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.

g) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario.

h) El comienzo y el fin del período de validez del certificado.

i) Los límites de uso del certificado, si se prevén.

j) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

2. La consignación en el certificado de cualquier otra información relativa al signatario, requerirá su consentimiento expreso.

Artículo 9. Vigencia de los certificados.

1. Los certificados de firma electrónica quedarán sin efecto, si concurre alguna de las siguientes circunstancias:

a) Expiración del período de validez del certificado.

Tratándose de certificados reconocidos, éste no podrá ser superior a cuatro años, contados desde la fecha en que se hayan expedido.

b) Revocación por el signatario, por la persona física o jurídica representada por éste o por un tercero autorizado.

c) Pérdida o inutilización por daños del soporte del certificado.

d) Utilización indebida por un tercero.

e) Resolución judicial o administrativa que lo ordene.

f) Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.

g) Cese en su actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del signatario, los certificados expedidos por aquél sean transferidos a otro prestador de servicios.

h) Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.

2. La pérdida de eficacia de los certificados, en los supuestos de expiración de su período de validez y de cese de actividad del prestador de servicios, tendrá lugar desde que estas circunstancias se produzcan. En los demás casos, la extinción de la eficacia de un certificado surtirá efectos desde la fecha en que el prestador de servicios tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en su Registro de certificados al que se refiere el artículo 11.e).

3. En cualquiera de los supuestos indicados, el prestador de servicios de certificación, habrá de publicar la extinción de eficacia del certificado en el Registro al que se refiere el artículo 11.e), y responderá de los posibles perjuicios que se causen al signatario o a terceros de buena fe, por el retraso en la publicación. Corresponderá al prestador de servicios la prueba de que los terceros conocían las circunstancias invalidantes del certificado.

4. El prestador de servicios de certificación podrá suspender, temporalmente, la eficacia de los certificados expedidos, si así lo solicita el signatario o sus representados o lo ordena una autoridad judicial o administrativa. La suspensión surtirá efectos en la forma prevista en los dos apartados anteriores.

Artículo 10. Equivalencia de certificados.

Los certificados que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro de la Unión Europea, de acuerdo con la legislación de éste, expidan como reconocidos, se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumplan alguna de las siguientes condiciones:

a) Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica y haya sido acreditado, conforme a un sistema voluntario establecido en un Estado miembro de la Unión Europea.

b) Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica.

c) Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

CAPITULO III

Condiciones exigibles a los prestadores de servicios de certificación

Artículo 11. Obligaciones de los prestadores de servicios de certificación.

Todos los prestadores de servicios de certificación deben cumplir las siguientes obligaciones:

a) Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho. Se exceptúan de esta obligación, los prestadores de servicios de certificación que, expidiendo certificados que no tengan la consideración de reconocidos, se limiten a constatar determinadas circunstancias específicas de los solicitantes de aquéllos.

b) Poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica.

c) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite.

d) Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial.

e) Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o perdida de vigencia de sus efectos. A dicho registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario.

f) En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo con la antelación indicada en el apartado 1 del artículo 13, a los titulares de los certificados por ellos emitidos y, si estuvieran inscritos en él, al Registro de Prestadores de Servicios del Ministerio de Justicia.

g) Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.

h) Cumplir las demás normas previstas, respecto de ellos, en este Real Decreto-ley y en sus normas de desarrollo.

Artículo 12. Obligaciones exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos.

Además de cumplir las obligaciones establecidas en los artículos 7 y 11, los prestadores de servicios de certificación que expidan certificados reconocidos, han de cumplir las siguientes:

a) Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.

b) Demostrar la fiabilidad necesaria de sus servicios.

c) Garantizar la rapidez y la seguridad en la prestación del servicio. En concreto, deberán permitir la utilización de un servicio rápido y seguro de consulta del Registro de certificados emitidos y habrán de asegurar la extinción o suspensión de la eficacia de éstos de forma segura e inmediata.

d) Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

e) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

f) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación.

g) Disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en este Real Decreto-ley y, en particular, para afrontar el riesgo de la responsabilidad por daños y perjuicios. Para ello, habrán de garantizar su responsabilidad frente a los usuarios de sus servicios y terceros afectados por éstos. La garantía a constituir podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un seguro de caución.

Inicialmente, la garantía cubrirá, al menos, el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada

prestador de servicios de certificación. Teniendo en cuenta la evolución del mercado, el Gobierno, por Real Decreto, podrá reducir el citado porcentaje, hasta el 2 por 100.

En caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de los certificados que emita el prestador de servicios de certificación, la garantía a constituir, cubrirá, al menos, su responsabilidad por un importe de 1.000.000.000 de pesetas (6.010.121,04 euros). El Gobierno, por Real Decreto, podrá modificar el referido importe.

h) Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años. Esta actividad de registro podrá realizarse por medios electrónicos.

i) Antes de expedir un certificado, informar al solicitante sobre el precio y las condiciones precisas de utilización del certificado. Dicha información, deberá incluir posibles límites de uso, la acreditación del prestador de servicios y los procedimientos de reclamación y de resolución de litigios previstos en las leyes y deberá ser fácilmente comprensible. Estará también a disposición de terceros interesados y se incorporará a un documento que se entregará a quien lo solicite. Para comunicar esta información, podrán utilizarse medios electrónicos si el signatario o los terceros interesados lo admiten.

j) Utilizar sistemas fiables para almacenar certificados, de modo tal que:

1. Sólo personas autorizadas puedan consultarlos, si éstos únicamente están disponibles para verificación de firmas electrónicas.

2. Unicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones.

3. Pueda comprobarse la autenticidad de la información.

4. El signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambios técnicos que afecten a los requisitos de seguridad mencionados.

k) Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando este Real Decreto-ley y sus disposiciones de desarrollo, en el ejercicio de su actividad.

Artículo 13. Cese de la actividad.

1. El prestador de servicios de certificación que vaya a cesar en su actividad, deberá comunicarlo a los titulares de los certificados por él expedidos y transferir, con su consentimiento expreso, los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios que los asuma o dejarlos sin efecto. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

2. Si el prestador de servicios estuviere inscrito en el Registro de Prestadores de Servicios de Certificación del Ministerio de Justicia, deberá comunicar a éste, con la antelación indicada en el anterior apartado, el cese de su actividad, y el destino que vaya a dar a los certificados

especificando, en su caso, si los va a transferir y a quién o si los dejará sin efecto. Igualmente, indicará cualquier otra circunstancia relevante, que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de un procedimiento de quiebra o suspensión de pagos respecto de él.

3. La inscripción del prestador de servicios de certificación en el Registro de Prestadores de Servicios de Certificación será cancelada, de oficio, por el Ministerio de Justicia, cuando aquél cese en su actividad. El Ministerio de Justicia se hará cargo de la información relativa a los certificados que se hubieren dejado sin efecto por el prestador de servicios de certificación, a efectos de lo previsto en el artículo 12.h).

Artículo 14. Responsabilidad de los prestadores de servicios de certificación.

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone este Real Decreto-ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.

2. El prestador de servicios de certificación sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

3. La responsabilidad será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, con las especialidades previstas en este artículo. Cuando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros.

4. Lo dispuesto en este artículo, se entiende sin perjuicio de lo establecido en la legislación sobre protección de los consumidores y usuarios.

Artículo 15. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y el que se realice en el Registro de Prestadores de Servicios de Certificación al que se refiere este Real Decreto-ley, se sujetan a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en las disposiciones dictadas en su desarrollo. El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.

2. Los prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o

con su consentimiento explícito. Los datos requeridos serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.

3. Los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, deberán constatar su verdadera identidad y conservar la documentación que la acredite. Dichos prestadores de servicios estarán obligados a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica 5/1992, de 29 de octubre. Ello se entiende sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

En todo caso, se estará a lo previsto en las normas sobre protección de datos indicadas en el apartado 1 de este artículo.

CAPITULO IV

Inspección y control de la actividad de los prestadores de servicios de certificación

Artículo 16. Supervisión y control.

1. El Ministerio de Fomento controlará, a través de la Secretaría General de Comunicaciones, el cumplimiento, por los prestadores de servicios de certificación que expidan al público certificados reconocidos, de las obligaciones establecidas en este Real Decreto-ley y en sus disposiciones de desarrollo. Asimismo, vigilará el cumplimiento, por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones establecidas en el artículo 11.

2. En el ejercicio de su actividad de control, la Secretaría General de Comunicaciones actuará de oficio, mediante petición razonada del Ministerio de Justicia o de otros órganos administrativos o a instancia de persona interesada. Los funcionarios de la Secretaría General de Comunicaciones adscritos a la Inspección de las Telecomunicaciones, a efectos de cumplir las tareas de control, tendrán la consideración de autoridad pública.

3. Cuando, como consecuencia de una actuación inspectora, se tuviera constancia de la contravención en el tratamiento de datos, de lo dispuesto en el artículo 11.c), la Secretaría General de Comunicaciones pondrá el hecho en conocimiento de la Agencia de Protección de Datos. Esta podrá, con arreglo a la Ley Orgánica 5/1992, iniciar el oportuno procedimiento sancionador, con arreglo a la legislación que regula su actividad.

Artículo 17. Deber de colaboración.

Los prestadores de servicios de certificación tienen la obligación de facilitar a la Secretaría General de Comunicaciones toda la información y los medios precisos para el ejercicio de sus funciones y la de permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, referida siempre a datos que conciernan al prestador de servicios.

Artículo 18. Resoluciones del órgano de supervisión.

La Secretaría General de Comunicaciones podrá ordenar a los prestadores de servicios de certificación la adopción de las medidas apropiadas para exigirles que cumplan este Real Decreto-ley y sus disposiciones de desarrollo.

TITULO III

Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

CAPITULO UNICO

Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

Artículo 19. Dispositivos seguros de creación de firma electrónica.

A efectos del artículo 2 f), para que se entienda que el dispositivo de creación de una firma electrónica es seguro, se exige:

1.º Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.

2.º Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.

3.º Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.

4.º Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

Artículo 20. Normas técnicas.

1. Se presumirá que los productos de firma electrónica que se ajusten a las normas técnicas cuyos números de referencia hayan sido publicados en el "Diario Oficial de las Comunidades Europeas" son conformes con lo previsto en la letra e) del artículo 12 y en el artículo 19.

2. Sin perjuicio de esta presunción, los números de referencia de esas normas se publicarán en el "Boletín Oficial del Estado".

Artículo 21. Evaluación de la conformidad con la normativa aplicable de los dispositivos seguros de creación de firma electrónica.

1. Los órganos de certificación a los que se refiere el artículo 6 podrán certificar los dispositivos seguros de creación de firma electrónica, previa valoración de los informes técnicos emitidos sobre los mismos, por entidades de evaluación acreditadas.

En la evaluación del cumplimiento de los requisitos previstos en el artículo 19, las entidades de evaluación podrán aplicar las normas técnicas respecto de los productos de firma electrónica a las que se refiere el artículo anterior u otras que determinen los órganos de acreditación y de certificación, y cuyas referencias se publiquen en el "Boletín Oficial del Estado".

2. Se reconocerá eficacia a los certificados sobre dispositivos seguros de creación de firma que hayan sido expedidos por los organismos designados para ello por los Estados miembros de la Unión Europea, cuando pongan de manifiesto que dichos dispositivos cumplen los requisitos contenidos en la normativa comunitaria sobre firma electrónica.

Artículo 22. Dispositivos de verificación de firma.

1. Los dispositivos de verificación de firma electrónica avanzada deben garantizar lo siguiente:

1. Que la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente.

2. Que el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

3. Que figura correctamente la identidad del signatario o, en su caso, consta claramente la utilización de un seudónimo.

4. Que se verifica de forma fiable el certificado.

5. Que puede detectarse cualquier cambio relativo a su seguridad.

2. El Real Decreto al que se refiere el artículo 6 podrá establecer los términos en los que las entidades de evaluación y los órganos de certificación podrán evaluar y certificar, respectivamente, el cumplimiento, por los dispositivos de verificación de firma electrónica avanzada, de los requisitos establecidos en este artículo.

TITULO IV

Tasa por el reconocimiento de acreditaciones y certificaciones

CAPITULO UNICO

Tasa por el reconocimiento de acreditaciones y certificaciones

Artículo 23. Régimen aplicable a la tasa.

1. La gestión precisa para el reconocimiento de las acreditaciones y de las certificaciones con arreglo a los artículos 6, 21 y 22, por los órganos públicos competentes, se grava con una tasa, a la que se aplicará el siguiente régimen:

a) Constituye el hecho imponible el reconocimiento por dichos órganos de la acreditación de los prestadores de servicios o de la certificación de los dispositivos de creación o de verificación de firma a que se refieren los artículos 6, 21 y 22.

b) Es sujeto pasivo la persona natural o jurídica que se beneficie del reconocimiento de la correspondiente acreditación o certificación.

c) Su cuota es de 47.500 pesetas (285,48 euros) por cada acreditación

S. 761

One Hundred Sixth Congress of the United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Monday, the twenty-fourth day of January, two thousand

An Act

To facilitate the use of electronic records and signatures in interstate or foreign commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Signatures in Global and National Commerce Act".

TITLE I—ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE

SEC. 101. GENERAL RULE OF VALIDITY.

(a) IN GENERAL.—Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce—

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

(b) PRESERVATION OF RIGHTS AND OBLIGATIONS.—This title does not—

(1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form; or

(2) require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.

(c) CONSUMER DISCLOSURES.—

(1) CONSENT TO ELECTRONIC RECORDS.—Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever

is required) such information satisfies the requirement that such information be in writing if—

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement—

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer—

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record—

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

(2) OTHER RIGHTS.—

(A) PRESERVATION OF CONSUMER PROTECTIONS.—Nothing in this title affects the content or timing of any disclosure or other record required to be provided or made

available to any consumer under any statute, regulation, or other rule of law.

(B) VERIFICATION OR ACKNOWLEDGMENT.—If a law that was enacted prior to this Act expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt (whichever is required).

(3) EFFECT OF FAILURE TO OBTAIN ELECTRONIC CONSENT OR CONFIRMATION OF CONSENT.—The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

(4) PROSPECTIVE EFFECT.—Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer's withdrawal of consent. A consumer's withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record. Failure to comply with paragraph (1)(D) may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this paragraph.

(5) PRIOR CONSENT.—This subsection does not apply to any records that are provided or made available to a consumer who has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) ORAL COMMUNICATIONS.—An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.

(d) RETENTION OF CONTRACTS AND RECORDS.—

(1) ACCURACY AND ACCESSIBILITY.—If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that—

(A) accurately reflects the information set forth in the contract or other record; and

(B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

(2) EXCEPTION.—A requirement to retain a contract or other record in accordance with paragraph (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.

(3) ORIGINALS.—If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided,

(1) constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of such Act enacted by a State under section 3(b)(4) of such Act shall be preempted to the extent such exception is inconsistent with this title or title II, or would not be permitted under paragraph (2)(A)(ii) of this subsection; or

(2)(A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if—

(i) such alternative procedures or requirements are consistent with this title and title II; and

(ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures; and

(B) if enacted or adopted after the date of the enactment of this Act, makes specific reference to this Act.

(b) EXCEPTIONS FOR ACTIONS BY STATES AS MARKET PARTICIPANTS.—Subsection (a)(2)(A)(ii) shall not apply to the statutes, regulations, or other rules of law governing procurement by any State, or any agency or instrumentality thereof.

(c) PREVENTION OF CIRCUMVENTION.—Subsection (a) does not permit a State to circumvent this title or title II through the imposition of nonelectronic delivery methods under section 8(b)(2) of the Uniform Electronic Transactions Act.

SEC. 103. SPECIFIC EXCEPTIONS.

(a) EXCEPTED REQUIREMENTS.—The provisions of section 101 shall not apply to a contract or other record to the extent it is governed by—

(1) a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;

(2) a State statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or

(3) the Uniform Commercial Code, as in effect in any State, other than sections 1–107 and 1–206 and Articles 2 and 2A.

(b) ADDITIONAL EXCEPTIONS.—The provisions of section 101 shall not apply to—

(1) court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings;

(2) any notice of—

(A) the cancellation or termination of utility services (including water, heat, and power);

(B) default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;

(C) the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or

(D) recall of a product, or material failure of a product, that risks endangering health or safety; or

(3) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

(c) REVIEW OF EXCEPTIONS.—

(1) EVALUATION REQUIRED.—The Secretary of Commerce, acting through the Assistant Secretary for Communications and Information, shall review the operation of the exceptions in subsections (a) and (b) to evaluate, over a period of 3 years, whether such exceptions continue to be necessary for the protection of consumers. Within 3 years after the date of enactment of this Act, the Assistant Secretary shall submit a report to the Congress on the results of such evaluation.

(2) DETERMINATIONS.—If a Federal regulatory agency, with respect to matter within its jurisdiction, determines after notice and an opportunity for public comment, and publishes a finding, that one or more such exceptions are no longer necessary for the protection of consumers and eliminating such exceptions will not increase the material risk of harm to consumers, such agency may extend the application of section 101 to the exceptions identified in such finding.

SEC. 104. APPLICABILITY TO FEDERAL AND STATE GOVERNMENTS.

(a) FILING AND ACCESS REQUIREMENTS.—Subject to subsection (c)(2), nothing in this title limits or supersedes any requirement by a Federal regulatory agency, self-regulatory organization, or State regulatory agency that records be filed with such agency or organization in accordance with specified standards or formats.

(b) PRESERVATION OF EXISTING RULEMAKING AUTHORITY.—

(1) USE OF AUTHORITY TO INTERPRET.—Subject to paragraph (2) and subsection (c), a Federal regulatory agency or State regulatory agency that is responsible for rulemaking under any other statute may interpret section 101 with respect to such statute through—

(A) the issuance of regulations pursuant to a statute; or

(B) to the extent such agency is authorized by statute to issue orders or guidance, the issuance of orders or guidance of general applicability that are publicly available and published (in the Federal Register in the case of an order or guidance issued by a Federal regulatory agency).

This paragraph does not grant any Federal regulatory agency or State regulatory agency authority to issue regulations, orders, or guidance pursuant to any statute that does not authorize such issuance.

(2) LIMITATIONS ON INTERPRETATION AUTHORITY.—Notwithstanding paragraph (1), a Federal regulatory agency shall not adopt any regulation, order, or guidance described in paragraph (1), and a State regulatory agency is preempted by section 101 from adopting any regulation, order, or guidance described in paragraph (1), unless—

(A) such regulation, order, or guidance is consistent with section 101;

(B) such regulation, order, or guidance does not add to the requirements of such section; and

(C) such agency finds, in connection with the issuance of such regulation, order, or guidance, that—

(i) there is a substantial justification for the regulation, order, or guidance;

(ii) the methods selected to carry out that purpose—

(I) are substantially equivalent to the requirements imposed on records that are not electronic records; and

(II) will not impose unreasonable costs on the acceptance and use of electronic records; and

(iii) the methods selected to carry out that purpose do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.

(3) PERFORMANCE STANDARDS.—

(A) ACCURACY, RECORD INTEGRITY, ACCESSIBILITY.—Notwithstanding paragraph (2)(C)(iii), a Federal regulatory agency or State regulatory agency may interpret section 101(d) to specify performance standards to assure accuracy, record integrity, and accessibility of records that are required to be retained. Such performance standards may be specified in a manner that imposes a requirement in violation of paragraph (2)(C)(iii) if the requirement (i) serves an important governmental objective; and (ii) is substantially related to the achievement of that objective. Nothing in this paragraph shall be construed to grant any Federal regulatory agency or State regulatory agency authority to require use of a particular type of software or hardware in order to comply with section 101(d).

(B) PAPER OR PRINTED FORM.—Notwithstanding subsection (c)(1), a Federal regulatory agency or State regulatory agency may interpret section 101(d) to require retention of a record in a tangible printed or paper form if—

(i) there is a compelling governmental interest relating to law enforcement or national security for imposing such requirement; and

(ii) imposing such requirement is essential to attaining such interest.

(4) EXCEPTIONS FOR ACTIONS BY GOVERNMENT AS MARKET PARTICIPANT.—Paragraph (2)(C)(iii) shall not apply to the statutes, regulations, or other rules of law governing procurement by the Federal or any State government, or any agency or instrumentality thereof.

(c) ADDITIONAL LIMITATIONS.—

(1) REIMPOSING PAPER PROHIBITED.—Nothing in subsection (b) (other than paragraph (3)(B) thereof) shall be construed to grant any Federal regulatory agency or State regulatory agency authority to impose or reimpose any requirement that a record be in a tangible printed or paper form.

(2) CONTINUING OBLIGATION UNDER GOVERNMENT PAPERWORK ELIMINATION ACT.—Nothing in subsection (a) or (b) relieves any Federal regulatory agency of its obligations under the Government Paperwork Elimination Act (title XVII of Public Law 105–277).

(d) AUTHORITY TO EXEMPT FROM CONSENT PROVISION.—

(1) IN GENERAL.—A Federal regulatory agency may, with respect to matter within its jurisdiction, by regulation or order issued after notice and an opportunity for public comment, exempt without condition a specified category or type of record from the requirements relating to consent in section 101(c) if such exemption is necessary to eliminate a substantial burden on electronic commerce and will not increase the material risk of harm to consumers.

(2) PROSPECTUSES.—Within 30 days after the date of enactment of this Act, the Securities and Exchange Commission shall issue a regulation or order pursuant to paragraph (1) exempting from section 101(c) any records that are required to be provided in order to allow advertising, sales literature, or other information concerning a security issued by an investment company that is registered under the Investment Company Act of 1940, or concerning the issuer thereof, to be excluded from the definition of a prospectus under section 2(a)(10)(A) of the Securities Act of 1933.

(e) ELECTRONIC LETTERS OF AGENCY.—The Federal Communications Commission shall not hold any contract for telecommunications service or letter of agency for a preferred carrier change, that otherwise complies with the Commission's rules, to be legally ineffective, invalid, or unenforceable solely because an electronic record or electronic signature was used in its formation or authorization.

SEC. 105. STUDIES.

(a) DELIVERY.—Within 12 months after the date of the enactment of this Act, the Secretary of Commerce shall conduct an inquiry regarding the effectiveness of the delivery of electronic records to consumers using electronic mail as compared with delivery of written records via the United States Postal Service and private express mail services. The Secretary shall submit a report to the Congress regarding the results of such inquiry by the conclusion of such 12-month period.

(b) STUDY OF ELECTRONIC CONSENT.—Within 12 months after the date of the enactment of this Act, the Secretary of Commerce and the Federal Trade Commission shall submit a report to the Congress evaluating any benefits provided to consumers by the procedure required by section 101(c)(1)(C)(ii); any burdens imposed on electronic commerce by that provision; whether the benefits outweigh the burdens; whether the absence of the procedure required by section 101(c)(1)(C)(ii) would increase the incidence of fraud directed against consumers; and suggesting any revisions to the provision deemed appropriate by the Secretary and the Commission. In conducting this evaluation, the Secretary and the Commission shall solicit comment from the general public, consumer representatives, and electronic commerce businesses.

SEC. 106. DEFINITIONS.

For purposes of this title:

(1) CONSUMER.—The term "consumer" means an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.

(2) ELECTRONIC.—The term "electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(3) ELECTRONIC AGENT.—The term "electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response.

(4) ELECTRONIC RECORD.—The term "electronic record" means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.

(5) ELECTRONIC SIGNATURE.—The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

(6) FEDERAL REGULATORY AGENCY.—The term "Federal regulatory agency" means an agency, as that term is defined in section 552(f) of title 5, United States Code.

(7) INFORMATION.—The term "information" means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(8) PERSON.—The term "person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

(9) RECORD.—The term "record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(10) REQUIREMENT.—The term "requirement" includes a prohibition.

(11) SELF-REGULATORY ORGANIZATION.—The term "self-regulatory organization" means an organization or entity that is not a Federal regulatory agency or a State, but that is under the supervision of a Federal regulatory agency and is authorized under Federal law to adopt and administer rules applicable to its members that are enforced by such organization or entity, by a Federal regulatory agency, or by another self-regulatory organization.

(12) STATE.—The term "State" includes the District of Columbia and the territories and possessions of the United States.

(13) TRANSACTION.—The term "transaction" means an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct—

(A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) services, and (iii) any combination thereof; and

(B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.

SEC. 107. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title shall be effective on October 1, 2000.

(b) EXCEPTIONS.—

(1) RECORD RETENTION.—

(A) IN GENERAL.—Subject to subparagraph (B), this title shall be effective on March 1, 2001, with respect to a requirement that a record be retained imposed by—

(i) a Federal statute, regulation, or other rule of law, or

(ii) a State statute, regulation, or other rule of law administered or promulgated by a State regulatory agency.

(B) DELAYED EFFECT FOR PENDING RULEMAKINGS.—If on March 1, 2001, a Federal regulatory agency or State regulatory agency has announced, proposed, or initiated, but not completed, a rulemaking proceeding to prescribe a regulation under section 104(b)(3) with respect to a requirement described in subparagraph (A), this title shall be effective on June 1, 2001, with respect to such requirement.

(2) CERTAIN GUARANTEED AND INSURED LOANS.—With regard to any transaction involving a loan guarantee or loan guarantee commitment (as those terms are defined in section 502 of the Federal Credit Reform Act of 1990), or involving a program listed in the Federal Credit Supplement, Budget of the United States, FY 2001, this title applies only to such transactions entered into, and to any loan or mortgage made, insured, or guaranteed by the United States Government thereunder, on and after one year after the date of enactment of this Act.

(3) STUDENT LOANS.—With respect to any records that are provided or made available to a consumer pursuant to an application for a loan, or a loan made, pursuant to title IV of the Higher Education Act of 1965, section 101(c) of this Act shall not apply until the earlier of—

(A) such time as the Secretary of Education publishes revised promissory notes under section 432(m) of the Higher Education Act of 1965; or

(B) one year after the date of enactment of this Act.

TITLE II—TRANSFERABLE RECORDS

SEC. 201. TRANSFERABLE RECORDS.

(a) DEFINITIONS.—For purposes of this section:

(1) TRANSFERABLE RECORD.—The term "transferable record" means an electronic record that—

(A) would be a note under Article 3 of the Uniform Commercial Code if the electronic record were in writing;

(B) the issuer of the electronic record expressly has agreed is a transferable record; and

(C) relates to a loan secured by real property.

A transferable record may be executed using an electronic signature.

(2) OTHER DEFINITIONS.—The terms "electronic record", "electronic signature", and "person" have the same meanings provided in section 106 of this Act.

(b) CONTROL.—A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

(c) CONDITIONS.—A system satisfies subsection (b), and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that—

(1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (4), (5), and (6), unalterable;

(2) the authoritative copy identifies the person asserting control as—

(A) the person to which the transferable record was issued; or

(B) if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;

(3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(4) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(5) each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

(6) any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

(d) STATUS AS HOLDER.—Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in section 1–201(20) of the Uniform Commercial Code, of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under the Uniform Commercial Code, including, if the applicable statutory requirements under section 3–302(a), 9–308, or revised section 9–330 of the Uniform Commercial Code are satisfied, the rights and defenses of a holder in due course or a purchaser, respectively. Delivery, possession, and endorsement are not required to obtain or exercise any of the rights under this subsection.

(e) OBLIGOR RIGHTS.—Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under the Uniform Commercial Code.

(f) PROOF OF CONTROL.—If requested by a person against which enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.

(g) UCC REFERENCES.—For purposes of this subsection, all references to the Uniform Commercial Code are to the Uniform Commercial Code as in effect in the jurisdiction the law of which governs the transferable record.

SEC. 202. EFFECTIVE DATE.

This title shall be effective 90 days after the date of enactment of this Act.

TITLE III—PROMOTION OF INTERNATIONAL ELECTRONIC COMMERCE

SEC. 301. PRINCIPLES GOVERNING THE USE OF ELECTRONIC SIGNATURES IN INTERNATIONAL TRANSACTIONS.

(a) PROMOTION OF ELECTRONIC SIGNATURES.—

(1) REQUIRED ACTIONS.—The Secretary of Commerce shall promote the acceptance and use, on an international basis, of electronic signatures in accordance with the principles specified in paragraph (2) and in a manner consistent with section 101 of this Act. The Secretary of Commerce shall take all actions necessary in a manner consistent with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce.

(2) PRINCIPLES.—The principles specified in this paragraph are the following:

(A) Remove paper-based obstacles to electronic transactions by adopting relevant principles from the Model Law on Electronic Commerce adopted in 1996 by the United Nations Commission on International Trade Law.

(B) Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced.

(C) Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.

(D) Take a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions.

(b) CONSULTATION.—In conducting the activities required by this section, the Secretary shall consult with users and providers of electronic signature products and services and other interested persons.

(c) DEFINITIONS.—As used in this section, the terms "electronic record" and "electronic signature" have the same meanings provided in section 106 of this Act.

TITLE IV—COMMISSION ON ONLINE CHILD PROTECTION

SEC. 401. AUTHORITY TO ACCEPT GIFTS.

Section 1405 of the Child Online Protection Act (47 U.S.C. 231 note) is amended by inserting after subsection (g) the following new subsection:

"(h) GIFTS, BEQUESTS, AND DEVISES.—The Commission may accept, use, and dispose of gifts, bequests, or devises of services or property, both real (including the use of office space) and personal, for the purpose of aiding or facilitating the work of the Commission. Gifts or grants not used at the termination of the Commission shall be returned to the donor or grantee.".

Speaker of the House of Representatives.

Vice President of the United States and
President of the Senate.