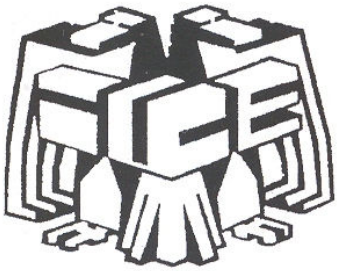


UNIVERSIDAD SALESIANA

ROL DEL NOTARIO PUBLICO EN LA FIRMA Y CERTIFICACION DIGITAL

T E S I S

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN DERECHO

P R E S E N T A :

ALMA LOURDES ALMAZAN REYES

MEXICO, D.F. 2006

Gracias a Dios por todo lo que me ha dado sin merecerlo,
y por que el ha ido trazando mi destino.

Con todo mi amor, dedicado este trabajo
y el de toda mi vida a mis Padres
con los que estoy eternamente agradecida
por su esfuerzo en darme educación.
Los amo.

A la Universidad Salesiana
donde encontré a las mejores personas
para una excelente formación
espiritual y profesional.

A amigos y amigas que seguro sí un día
volviera escoger mi destino
y si un día mis pasos se hicieran camino
quisiera que siempre estuvieran conmigo.

ROL DEL NOTARIO PUBLICO EN LA FIRMA Y CERTIFICACIÓN DIGITAL

INTRODUCCIÓN

CAPITULO I.- ANTECEDENTES HISTÓRICOS

CAPITULO II. MARCO LEGAL

CAPITULO III. DE LA FIRMA EN GENERAL

INTRODUCCIÓN

Son ya notables los cambios que se han producido en la nueva era de la Información. Algunos de los mayores impactos de la Tecnología de la Información se verifican en el comercio, los servicios financieros, los servicios del gobierno y el ámbito notarial no es la excepción. Ya que las funciones que los Fedatarios Públicos pueden ejercer en el mundo virtual, no son diversas de las que hoy ejercen en el mundo real, sólo se trata de herramientas distintas para hacerlo.

El presente trabajo, gira en torno de la firma y certificación digital y a los cambios que se observan, y que viven los notarios en el ejercicio de su función, así pues, trato de hacer un análisis del desarrollo de la firma desde sus orígenes y de todo el tiempo que tuvo que pasar para que el notario pueda hacer uso de la tecnología de hoy en día.

De lo anterior, es importante hacer referencia de la infraestructura desarrollada por algunos países y organismos internacionales, y en la manera en que éstos han hecho lo posible para permitir el funcionamiento de la firma y certificación digital, utilizada en la actualidad para otorgar seguridad a las transacciones comerciales, electrónicas y a la transferencia electrónica de datos, por tal razón los países y organismos tratan de ponerse al día para actualizar algunas de sus instituciones, sistemas, estructuras, y legislar en la materia para hacer más competitiva su legislación frente a otros países que se puedan

encontrar en el mismo supuesto, considerando dentro de ello, lo correspondiente al ámbito notarial.

En nuestro país, no nos hemos quedado atrás, ya que el aparato legislativo mexicano ha tomado con mucha cautela el hacer una legislación acorde a las necesidades que trae consigo esta nueva etapa de desarrollo tecnológico, y en el derecho especialmente en lo que se refiere al Notario y su función.

Me parece que lo verdaderamente importante, no viene del cuestionamiento de querer hacer uso de ella o no, si no en cómo afrontar el reto de su incorporación y capacitación para que puedan ser ejercidas en beneficio de la legalidad de la función notarial para aprovechar las ventajas competitivas que ésta provee.

A nadie ya escapa la velocidad y la voracidad con que avanza la tecnología; fundamentalmente en el tema que nos ocupa hago un análisis de cómo se han creado diferentes tecnologías para estudiar la firma digital, como la criptografía y todo lo que trae implicado el tema; el ámbito en que se aplica, los dispositivos de creación y verificación de la misma con un ligero vistazo en algunas implicaciones penales, teniendo como base los conceptos fundamentales, tanto de informática, como de derecho.

El tema de los agentes certificadores merece especial atención, ya que es donde realmente entra la función del notario, y donde se analiza la función

certificadora de la que éste goza, así como, las innovaciones de las que no sólo haría uso el notario, si no también, las instituciones de las cuales él depende, y las que son auxiliares de él, todo esto para que sea más eficaz el ejercicio de su fe pública, trayéndole nuevas y mejores opciones para crecer en su campo de actuación.

CAPITULO I

ANTECEDENTES HISTÓRICOS

1.1 Roma
- 1.1.1 Edad Media

1.2 España

1.3 Estados Unidos de Norte América

1.4 México
- 1.4.1 Época Precolonial
- 1.4.2 Época Colonial
- 1.4.3 México Independiente

1.5 Latinoamérica
- 1.5.1 Argentina
- 1.5.2 Chile
- 1.5.3 Colombia
- 1.5.4 Venezuela

1.6 Organismos Internacionales
- 1.6.1 UNICITRAL - CNUDMI
- 1.6.2 Comunidad Europea

CAPÍTULO I. ANTECEDENTES HISTÓRICOS

1.1 ROMA

No es fácil determinar el momento histórico en que alguien estampó su firma autógrafa y que además le fue reconocida con las implicaciones de la actualidad. Podemos hacer referencia desde la aparición del hombre cuando él aún no se comunicaba verbalmente, pero ya ideaba el cómo distinguir sus pocas pertenencias de las de los demás por medio de señas estampadas en ellas o por la forma especial de su manufactura; los bienes inmuebles se ostentaban basándose en el señorío, es decir, aquel que materialmente se manifestaba como dueño y le era reconocido por la tribu o familia; al pasar el tiempo el hombre se empieza a comunicar con dibujos y pinturas que fueron usados para crear figuras para usarlas a modo de emblemas el cual daba una especie de identificación o individualidad de un *paterfamilia,* o de una Tribu determinada, ya con los antecedentes de los dibujos y figuras el hombre fue simplificándolos hasta convertirlos en signos que representaban palabras cuya sistematización dío nacimiento a la escritura.

Entre el IV y III milenios antes de Cristo, diversos pueblos fundaron ciudades en donde florecieron las primeras civilizaciones, como los egipcios, fenicios, sumerio y cretense, el alfabeto de las dos primeras es muestra del adelanto en que vivían tales civilizaciones, aunque ya conocían la escritura, los dibujos y figuras siguieron siendo usadas, no solo durante el tiempo anterior a la

Era Cristiana sino hasta muy adelantada la Edad Media, pero esta etapa de la historia lo presentaré más adelante.

Aún con los pocos datos que existen sobre el uso de la firma en la antigua civilización helena, sí se puede llegar a determinar que si bien los griegos no usaban habitualmente la firma, ya que, "en Roma no se firmaban los documentos ni era costumbre ni necesario (Cod. Just. VII, 6, 1, Inst. III, 23)[1], pero por lo menos en materia de contratos "si existía una forma de dar seguridad a los contratantes, mediante una institución llamada el *ágora*, que era donde se desarrollaban las más importantes actividades de intercambio de productos, y el que servía como publicidad para darlos a conocer entre las gentes de la ciudad, en la que circulaban los inspectores llamados *agranomoi*, que se encargaban de vigilar el orden y honestidad en las transacciones." [2]

Aunque en la Segunda mitad del primer siglo de la Era Cristiana ya se identificaba jurídicamente a la persona física, pues así se evitaban los fraudes en los contratos (en especial el de compraventa que era el más común), así pues el gobierno romano de Egipto creó y organizó una institución llamada "Archivo de Posesiones" en el cual "se llevaba un registro en libros denominados *distromatas*, en donde se asentaban los derechos relativos a los bienes inmuebles y a esclavos pertenecientes a personas cuyo domicilio estuviese en los diferentes distritos administrativos de cada población, para obtener dicho registro el interesado hacía una petición, acompañada del documento que acreditaba la transacción, ésa inscripción, no era un requisito para la validez de la operación pero sí otorgaba

[1] ENCICLOPEDIA JURÍDICA OMEBA, Tomo XIII, Editorial Bibliográfica Fami-Gora, Argentina, 1974, p. 290.
[2] AHRENS, Enrique, *Historia del Derecho*, Editorial De Palma, Argentina, 1945, p. 111.

cierta protección a sucesivos adquirentes".[3]

En la ciudad de Alejandría, la que contaba con su propio sistema jurídico se encontró un papiro, al cual se le daba preferencia ya que en principio los documentos eran redactados en tablas que eran enceradas y unidas unas con otras, y en donde un tesorero asentaba las ventas por medio de inscripciones que no hacían mención de la firma o sellos, pero sí de la forma en que debía hacerse la identificación del vendedor y del comprador, tales inscripciones eran extendidas por un funcionario con carácter notarial llamado *Agranome,* el cual sólo declaraba que la transacción había sido realizada ante él y con ese objeto extendía un tipo de certificado, el cual no era válido si no llevaba su sello oficial, el que era considerado como un documento de legitimación para el adquirente.[4]

Para poder desarrollar los antecedentes histórico-jurídicos de la firma y otros signos como elementos de identificación y de manifestación de la voluntad del individuo dividiremos al derecho romano en tres grandes épocas.

1. - Derecho Antiguo, que comprende de la fundación de Roma al fin de la República (1 a 723 de Roma).

2. - Época Clásica del Derecho Romano del advenimiento del Imperio a la muerte de Alejandro Severo (723 de Roma a 225 de la Era Cristiana).

3. - Derecho del Bajo Imperio, que abarca de la muerte de Alejandro Severo a la muerte de Justiniano (225 a 565 de la Era Cristiana).

---

[3] ORTOLAN, José Luis, *Explicación histórica de las Instituciones del Emperador Justiniano* traducción (PÉREZ DE ANAYA Francisco), Editorial Hijos de Leocadio López, España, 1912, p. 118.

[4] FLORIS MARGADANT, Guillermo, *El derecho privado romano*, Editorial Esfinge, México, 1960, p. 378.

En el derecho Antiguo, podemos hacer referencia a la Ley de las 12 tablas[5] y es la etapa de infancia del derecho, a pesar de esto ya existía el contrato *literis* el que se efectuaba de las menciones escritas en el *Codex* del *paterfamilias* llamadas "*nomina transcripta*" el cual se perfeccionaba por la inscripción de una deuda en la contabilidad doméstica del *paterfamilias*, esas contabilidades tenían él carácter de sagradas, el *paterfamilias* pasaba los asientos del borrador (adversaria, libro diario) al *codex,* y por su solemnidad, tal vez esas inscripciones en el *codex* producían acción contra el deudor aunque éste no hubiera colaborado en el acto.[6]

El contrato *literis* se perfeccionaba por un acto unilateral del acreedor, era un contrato *stricti iuris ,* ya que era un acto relacionado con conceptos religiosos romanos, y por tal carácter sagrado, se protegía a deudores contra la mala fe del acreedor, el contrato también era válido sólo entre los ciudadanos romanos, entre un *paterfamilias* y sus clientes, por la relación con la contabilidad el objeto de los contratos *literis,* solo podían consistir en sumas de dinero, y la acción que le daba eficacia era la *condictio certae pecuniae* que ya se establecía en el caso de la *stipulatio* sobre cierta cantidad de dinero.

---

[5] Apuntes tomados en clase del Lic. Martín Aguilera Mendoza, *Introducción al Estudio del Derecho Romano*, Universidad Salesiana, México D.F, 1996. El derecho en principio se desarrolla con la interpretación de los pontífices y los jurisconsultos que eran los conocedores y peritos del derecho canónico y nacional, así nace la Ley de las 12 Tablas que adquirió un carácter de ley nacional y reglamentaron el derecho público y privado era como la base y fuente de su derecho, éstas se hicieron y fueron encomiendas a 10 patricios en el año 303 A.C. las que hicieron y publicaron hasta el 304, estos 10 eran llamados decinuros que hicieron las primeras 10 tablas posteriormente llaman a otro decinuro para las 2 restantes.

[6] FLORIS MARGADANT, Guillermo, *El derecho privado romano como introducción a la cultura jurídica contemporánea*, decimoquinta edición, Editorial Esfinge, México, 1988 p. 390.

Con el fin de la República y por el excesivo formalismo del derecho romano, no bastaba, salvo en casos excepcionales el consentimiento de las partes, sino que era necesario que los documentos se acompañarán de determinadas formalidades como la entrega de la cosa y la de pronunciar palabras solemnes, y durante todo el Bajo Imperio, es cuando comienzan a caer en desuso la religión doméstica y las contabilidades relacionadas con ella, ya en la Época Clásica encontramos a los documentos que lo sustituyeron al citado contrato: el *chirographa* y *singraphae* y que Justiniano denomina como documentos probatorios, de la existencia de contratos que se habían perfeccionado *verbis* es decir un préstamo formalizado por *stipulatio* o *re,* que era un préstamo en forma de mutuo. [7]

El *chirographa* era un verdadero compromiso del deudor de pagar una cierta cantidad de dinero, y por eso era firmado sólo por el deudor y sellado con un anillo que quedaba en poder del acreedor. El *singraphae* por su parte contenía los sellos del deudor y del acreedor con la firma de ambos el cual era redactado en dos ejemplares, y cada parte se quedaba con un tanto.

Gayo, luego atestiguó que este procedimiento era usado en su tiempo por los peregrinos que no se podían obligar mediante la *nomina transcripta* del *pater Familias* y que creaba una verdadera obligación literal, igualmente afirma que son documentos que servían para transformar una obligación preexistente y por lo tanto, eran simples instrumentos de novación.[8]

---

[7] Vid. PETIT, Eugene, *Tratado elemental de Derecho Romano*, Editorial Cárdenas Editor y Distribuidor, México, 1989, págs 277 a 352.
[8] Ibíd. págs 374 y 375.

Hay autores que creen que el *chirographa* no era más que un medio probatorio pero que nunca constituyó una fuente de obligaciones en el derecho romano. Sin embargo Eugene Pettit sostiene que "sí es una fuente de las obligaciones ya que así lo establecen los textos legales de la época y por la existencia de una excepción no tendría razón de ser en caso de no constituir estos documentos una fuente de las obligaciones, esta era la excepción *non numerata pecuniae*".[9] Nos parece, que esta es la opinión más adecuada a la realidad jurídica de esa época por que como sabemos los romanos ya conocían la existencia de los actos y hechos jurídicos considerándolos como la causa del derecho (como fuente que los origina), así mismo distinguían entre ambos; a los hechos como acontecimientos que se causan independientemente de la voluntad del hombre y a los actos o negocios jurídicos como acciones derivadas de la voluntad del hombre, donde intervenía por supuesto el consentimiento**;** esto sólo para hacer referencia de los elementos necesarios en un contrato y tema que será tratado más ampliamente en posteriores capítulos.

Como ya dijimos antes, en Roma no era necesario ni costumbre firmar los documentos, ya que el uso de la firma o huella digital era nulo, todo parece indicar que lo único que las sustituía era un sello. Así que tuvieron que hacer uso de la *manufirmatio***,** que "consistía en una ceremonia en que leído el documento por su autor o el notario se colocaba desenrollado y extendido sobre la mesa del escribano y luego de pasar la mano abierta sobre el pergamino en actitud de jurar pero sin hacerlo, se estampaba el nombre, signo, una o tres cruces –una por cada persona de la Santísima Trinidad- por el autor o notario en su nombre haciéndolo

[9] Ídem

seguidamente los testigos". [10] Más que un requisito, la *manufirmatio* era en si misma una parte del espectáculo solemne en que se realizaba el acto.

En aquel tiempo ya se hablaba de autenticar los documentos con signos y sellos, pero con el desenvolvimiento de las transacciones comerciales principalmente la firma fue adquiriendo la importancia y concepción que actualmente tiene.

1.1.1 Edad Media

Esta etapa representa un período muy importante en el desarrollo de la firma ya que en esta etapa de la historia se adquiere la costumbre entre gobernantes, que para autentificar documentos se usarán a modo de firma marcas, sellos y signos, estos últimos al pasar del tiempo fueron dando lugar a lo que ahora se conoce como rúbrica**,** pero en esa época, estos signos eran formados por una cruz con la que se entrelazaban en forma arbitraria, letras o rasgos, y que fueron usados por los fedatarios hasta hace no mucho. Así que "los cristianos adoptaron la costumbre de trazar una cruz como signo de firma" [11]

Durante el reinado de Carlo Magno, éste hacía firmar sus actos por un sellero oficial, lo mismo hicieron sus sucesores, que siguieron usando sellos hasta que algún tiempo después comenzaron a autenticarse los documentos con sello y

---

[10] ENCICLOPEDIA JURÍDICA OMEBA, op cit, págs 290 y 291.
[11] GRAN ENCICLOPEDIA LAROUSSE, Tomo IV, Editorial Planeta, S.A., México, 1972 p 86.

firma aunque por eso se entendían todavía los signos dibujados para individualizarse.[12]

En 1358 Carlos V obligó en Francia, a que los escribanos suscribieran los actos que pasaban ante ellos con sus firmas además de sus signos en ese mismo año en El Consejo Real el Rey, dispuso que los actos de ese organismo debían de ser autorizados por lo menos por tres de los presentes mediante firma, en caso de no saber firmar estamparían sus marcas o signos.[13]

La diferencia entre firmas y signos, hizo que empezase a entender que las primeras eran más que sólo signos, ya que podía interpretarse como la inscripción manuscrita del nombre o de los apellidos, ya con el pasar del tiempo y con el aumento de las transacciones comerciales hicieron que la firma fuera adquiriendo tal importancia que fue consagrando como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona.

Así que a partir de la Edad Media, se desarrollan modificaciones en lo que a medios y formas de plasmar el consentimiento se refiere, podríamos referir tal desarrollo en 3 etapas, la primera de ellas del s. V al IX, en la Época Medieval donde se usaba el pergamino como el medio más común para escribir y con él permaneció la extensión y uso del sello, entre gobernantes, funcionarios y pequeños terratenientes.

Los sellos y documentos (estos con relación a su contenido) presentaban algunas variantes de acuerdo a la persona que los emitía, es decir había sellos reales, religiosos, municipales y comerciales. También en ésta época el derecho

---

[12] TOMAS Y VALIENTE, Francisco, *El orden Jurídico Medieval*, Editorial Marcial Pons Ediciones Jurídicas y Sociales S.A., España, 1996, págs 53-54.
[13] ENCICLOPEDIA JURÍDICA OMEBA, op cit, págs 290-291.

Germánico introdujo ciertos formalismos simbólicos diferentes de los del Derecho Romano y el Derecho Canónico, proclamando el valor del consentimiento, es decir un verdadero con sensualismo ya que los primeros años de la Edad Media (s. V al VIII) se da una ruptura del contrato como tal, así que, las relaciones contractuales se basaron en las armas y la confianza que eran los únicos elementos de consentimiento que daban validez al contrato.[14]

Un ejemplo de lo anterior, se da en España durante la influencia del Derecho Canónico, donde se encuentra una nota acentuada de con sensualismo, en la ley única, del Ordenamiento de Alcalá que establece "Pareciendo que alguno se quiso obligar a otro por promisión o por algún otro contrato o en otra manera; sea tenido de cumplimiento aquello que obligó y no puede poner excepción, que no fue hecha estipulación que quiere decir prometimiento con cierta solemnidad de derecho mandamos que todavía haya dicha obligación y contrato que fueren hechos en cualquier manera que parezca que uno se quiso obligar a otro"[15]

Con lo anterior, se apunta el formalismo de los contratos y pasa a un simple summun del con sensualismo por lo que los contratos serían obligatorios cualquiera que fuere la condición en que se hubiesen celebrado, siempre y cuando hubieren concurrido las condiciones esenciales para tener validez.[16]

Ya en la segunda etapa de la Edad Media, es decir a partir del s. IX, la iglesia católica que es organizada en torno a una estructurada jerarquía con el

---

[14] FLORIS MARGADANT, Guillermo, *Panorama de la Historia Universal del Derecho*, 1a Reimpresión, Editorial Porrua, México, 2002, p. 139.
[15] ROMERO, José Luis, *La edad Media*, Editorial FCE, México, 1994, p 39.
[16] BORJA SORIANO, Manuel, *Teoría General de las obligaciones*, Editorial Porrua, México, 1998, p 184.

Papa como indiscutida cúspide, se hace importante el uso del sello papal como equivalente de la firma y por ende de la exteriorización de la voluntad.[17]

Comenzó el uso de las Bulas papales,[18] en consecuencia de las tierras descubiertas por el Rey Alfonso V, de Portugal, y los Reyes Católicos españoles que solicitaron al Papa su intervención para que estableciera los derechos y beneficios sobre las tierras descubiertas, y en algunos casos las Bulas también limitaban derechos para futuras exploraciones, un ejemplo de ésta es la Bula Aeterni Regis (1481), que delimitaba la zona de expansión de los reinos peninsulares, o la Bula Alejandrina (1493), que con la noticia del éxito colombino y ante las pretensiones de Juan II, se solicitó al Papa Alejandro VI reconociera el derecho de los Reyes Católicos sobre los descubrimientos de las Indias.

Por último, la tercera etapa de la Edad Media, se puede caracterizar primero por el incremento de nuevas tierras descubiertas y segundo por que surge el Renacimiento, que como sabemos nace en Italia en el s. XIV y se difundió en el resto de Europa en los s. XV y XVI, en ésta etapa es cuando se inventa la imprenta y como consecuencia se difunde más el conocimiento, y es también cuando decayó el uso del pergamino. Así que el uso de sellos continuo siendo

---

[17] FLORIS MARGADANT, Guillermo, op cit, págs 145 a 148.

[18] Bula "carta especial de la Iglesia Católica relativa a materia de fe o cuestiones generales que lleva sello del Papa, y así también eran denominados los documentos en el que realizaba la impresión, el término Bula es exclusivo de la figura del Papa en oposición a los documentos del Estado que llevan el membrete real el sello pontificial se encuentra impreso en la mayoría de las Bulas, el cual lleva estampado el nombre del Papa y las cabezas de San Pedro y San Pablo, hasta el s. XI, las Bulas pontificias se escribían en papiro, luego en pergamino, las ya mencionada bulas tiene su auge durante el s. XV en el Renacimiento" Ídem.

común incluso en China y Japón que usaron los sellos para confirmar una firma o para identificar posesiones.

También siguieron siendo usadas las Bulas papales las cuales versaban sobre los descubrimientos de nuevas tierras, y como consecuencia nace un nuevo documento llamado Capitulación en el que se estableció una nueva relación comercial entre el Estado y un particular, un ejemplo de estos documentos es la Capitulación de Santa Fe (1492) realizada entre los Reyes Católicos Españoles y Cristóbal Colon.[19]

1.2. ESPAÑA

En este país encontramos que a partir de la Ley de Partidas, en el Fuero Juzgo (cuyo autor como sabemos es Alfonso X el Sabio también autor de leyes como el Fuero Real y las Siete Partidas, durante el siglo XIII al siglo XV. En este período es cuando se determina la función pública de los notarios), en el Fuero Real y en las Leyes del Toro, ya existía reglamentación acerca de la firma, la rúbrica y el estampado de sellos, sin embargo aunque en gran cantidad de textos legales se habla de la firma ninguno de ellos la define.

En la Ley de Partidas la Ley 54,Titulo XVIII, Partida 3ª, disponía que al final de las cartas aparecieran los nombres de los testigos con el nombre y signo del escribano: “como deben ser fechas las notas de las cartas de los escribanos públicos... En toda carta que sea fecha por mano del escribano público, deben ser puestos los nombres de aquellos que las manden facer...” Al referirse al escribano

[19] MIRANDA, José, *Historia de México,* 12ª Edición, Editorial Porrua, México, 1983, p. 177-188.

y a la nota que debiera asentar dice: “así como dice en ella e por ruego, e por mandato de los, escribí esta carta pública, y puse en ella mío signo e escribí mío nome”.[20] Obligando este mismo Código al escribano a inscribir sus notas en un libro conocido como Registro, en donde se hacía una remembranza de los hechos de cada año.

Dentro de esta legislación, se preveían los casos de no poder o no saber firmar, no sólo de los otorgantes si no también de las personas que servían de testigos y en materia de testamentos, la Ley I. Título I. De la Partida 6ª, exigía la firma del testador y los testigos diciendo: “. . . cada uno de ellos debe escribir su nome en el fin del testamento, diciendo así: yo sutano, so testigo deste testamento, que lo fizo tal ome seyendo yo presente. E si alguno dellos non supiere escribir quialquiera de los otro lo puede fazae por mandado del.... otro-si, dezimos que el facedor del testamento debe escribir su nimeen fin de la carta, diciendo así: yo fulano otorgo que fize este testamento en la manera que es escrito en esta carta. E si non supiese o non pudiese escribir, bien lo puede fazer otro por mandado del.” [21]

También la ley 3ª de las Leyes de Toro exigía la presencia y firma de los testigos, testador y del notario ” ....pero en el testamento cerrado que en latín se dice in-scriptis, mandamos que intervengan a lo menos siete testigos con un escribano: los cuales hayan de firmar . . . de manera que sean ocho firmas y el signo del escribano....” y además dice “si no tuvieren la dicha solemnidad de

---

[20] BERNI Y CATALA, Joseph D. Dr., *Apuntamientos sobre las Leyes de Partidas al tenor de leyes recopiladas, autos acordados, autores españoles y prácticas modernas*, Editorial Imprenta de Benito Monfort, España, 1759, p 143.

[21] LOS CÓDIGOS ESPAÑOLES CONCORDADOS Y ANOTADOS, Editorial Imprenta La Publicidad, España, 1850, p 2.

testigos mandamos, que no haga fe ni prueba en juicio ni fuera del". También esta ley establece la nulidad del documento que no reúna los requisitos establecidos en ella.[22]

En el Fuero Real que nace en 1255, exigía que los documentos fueran autorizados por escribanos y escritos por ellos mismos, además establecía entre otras cosas la obligación de otorgar testamento ante el escribano, así se instituía que: " más cada uno haga las cartas con su mano" y que pusieran su signo, "e todas las cartas que ficiese el Escribano mata e su señal conocida, por que puede ser sabida e conocida la carta qual escribano la fizo". [23] En esta disposición no se considera a la firma como un acto de voluntad sino que sólo servía para identificar en un momento determinado al escribano que la había redactado, considerando a este como un auxiliar de los intereses de los particulares; acostumbrándose que tomaran nota de los documentos que redactaban, o de aquellos en que intervenían.

En la Pragmática de Alcalá (en 1348 surgió el Ordenamiento de Alcalá en Alcalá de Henares dado por el Rey Don Alfonso XI, con el cual se buscaba coordinar las leyes y conciliar los sistemas de costumbres jurídicas de la época), esta exigía sólo la firma de las partes diciendo "... y si las partes otorgaren, la firmen de sus nombres y si no supieren firmar, firmen por ellos cualquiera de los testigos, otro que sepa escribir el cual escribano haga mención como el testigo firmo por la parte que no sabia hacerlo". Como se ve en esta disposición se prevé el caso de que las partes no puedan firmar, y aún cuando ésta no es

[22] BERNI Y CATALA, Joseph, op cit, p 396.
[23] ENCICLOPEDIA JURÍDICA ESPAÑOLA T. XVI, Editorial Francisco Seix Editor, España 1910, p 403.

absolutamente novedosa, pues ya lo vimos al referimos a los testamentos en la Ley de Partidas que era posible tal sustitución de firmas en caso de que se hicieran ante notarios, pero en materia de contratos y demás disposiciones ínter vivos si es un gran adelanto en materia de firmas. Sin embargo, la Pragmática de Alcalá no exige ni la firma de los testigos ni la del escribano, bastando que éste último firmara al cierre del protocolo al final del año, quedando así solemnizado todo el protocolo.[24]

Posteriormente debido a una diversidad de prácticas entre los notarios se estableció por medio de la Real Orden 1868, que era necesaria en las escrituras matrices, la firma de los testigos instrumentales o de conocimiento previendo desde luego el caso de que alguno de los testigos o de los contrayentes no supiese firmar. El reglamento de 1874 complementa lo anterior aclarando que; los actos y contratos entre vivios que sean firmados por los otorgantes y si estos o alguno de ellos no supiera o no pudiera firmar lo expresara así el notario y firmara un testigo por el que no lo haga, manifestándolo así el notario en el acta, años más adelante lo anterior lo contemplo la Ley del Notariado, estableciendo que serán nulos los instrumentos públicos donde no aparezcan las firmas de las partes incluyendo las de los testigos, cuando deban hacerlo.[25] Cabe señalar, que esta ley no menciona a que clase de nulidad está sujeta tales instrumentos ni especifica de que manera se puede purgar el vicio.

También en el Código Civil Español en la Sección Primera, que trata de los documentos públicos y privados establece en su artículo 1216 que “son

---

[24] ENCICLOPEDIA JURÍDICA ESPAÑOLA, Ibíd. p 404.
[25] Ídem

documentos públicos los autorizados por un notario o empleado público competente, con las solemnidades requeridas por la ley", refiriéndose a la solemnidad de la firma; y más adelante en él artículo 1229 que trata de los documentos privados dice "La nota escrita o firmada por el acreedor a continuación, al margen o al dorso de una escritura que obre en su poder, hace prueba en todo lo que sea favorable al deudor. Lo mismo se entenderá de la nota escrita o firmada por el acreedor al dorso, al margen o a continuación del duplicado de un documento o recibo que se halle en poder del deudor....." [26]

Como vemos ésta legislación ya hacía referencia de la firma como tal e iba más allá, y ya lo utilizaba para referirse a los documentos públicos aplicándolo en ciertos casos para hacer prueba en caso de alguna controversia.

La legislación actual y la jurisprudencia de este país han pensado en que por razones de seguridad y para ofrecer mayor confianza a los usuarios y jueces que a la postre deben juzgar sobre la firma digital, una reforma de ley cuyo objetivo fuera equiparar la firma manuscrita a cualquier otro medio de firma, que cumplirá con las mismas finalidades, sería una medida positiva.

Los antecedentes de lo anterior, se encuentran en la Circular del Banco de España No. 8/88 de 14 de junio de 1988, en la que se crea el reglamento del Sistema Nacional de Compensación Electrónica, la que se convirtió en pionera, y marco un hito para la protección y seguridad necesaria en la identificación para el acceso a la información, al indicar que la información se cifrara, para que las entidades introduzcan un dato de autenticación con la información de cada

[26] CÓDIGO CIVIL ESPAÑOL, 2a Edición, Colección de Textos Jurídicos, Bosch Casa Editorial, España 1989. p 54.

comunicación, a lo que se le reconoce el mismo valor que el que posee un escrito firmado de puño y letra.[27]

El Real Decreto 263/1996 de 16 de febrero de 1996, indica que deberán adoptarse las medidas técnicas que garanticen la identificación y la autenticidad de la voluntad, pero aún no hacia ninguna regulación legal acerca de la firma electrónica.[28]

Asimismo, el Real Decreto del 17 de septiembre pero de 1998, reconoció el uso de la firma electrónica, su eficacia jurídica y la prestación al público de servicios de certificación. El 17 de noviembre, del mismo año, durante las jornadas de Comercio Electrónico de la FECEMD Federación de Comercio Electrónico y Marketing Directo, se anuncia que casi toda la Ley sobre firma electrónica es aplicable directamente, pero que aún resta un pequeño porcentaje, en el que se incluye la acreditación de las entidades certificadoras las que exigen un breve reglamento.[29]

El más importante antecedente español se encuentra en el Real Decreto Ley 14/1999 del 17 de septiembre de 1999, que después fue derogado por la Ley 59/2003, de 19 de diciembre de 2003, [30] y en donde además de regular el uso de la firma electrónica, dicha Ley también define diversos conceptos como el de:

---

[27] MARTÍNEZ NADAL APOL-LONIA, *Ley de Firma Electrónica*, 2a edición, Editorial Civitas, serie civitas monografías, España 2001, págs 28 a 35.
[28] Ídem.
[29] Ídem.
[30] Ministerio de Industria, Turismo y Comercio, Real Decreto-Ley 14/1999 de 17 de septiembre, sobre firma electrónica, (derogada por Ley 59/2003, de firma electrónica). [En línea]. Disponible: http://wwwsetsi.mcyt.es/legisla/internet/rdley14_99.htm, 14 abril de 2006.

- Firma Electrónica: “es el conjunto de datos en forma electrónica, ajenos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge”;

Además hace la distinción entre la anterior y la firma electrónica avanzada a la que define como:

- Firma electrónica avanzada: “es la Firma Electrónica que permite la identificación del signatario y ha sido creada por medios que este 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 estos datos”.

Como podemos apreciar en lo que respecta a la firma digital, esta es considerada como firma electrónica avanzada y cuenta con los requisitos de integridad e inalterabilidad del documento.

Con relación a los certificados en el supuesto de empezar a prestar estos servicios de certificación, se establece un régimen de libre competencia requiriendo de la autorización previa del Registro de Prestadores de Servicios de Certificación, que depende del Ministerio de Justicia, estableciendo un sistema voluntario de acreditación de firma electrónica permitiendo lograr un cierto grado de seguridad.[31]

Esta Ley regulará el uso de la firma electrónica, mediante la cual se creará un vínculo de confianza entre usuarios gracias a la utilización de servicios de certificación dándole un respaldo jurídico a la firma. Con esto, se equipara la firma

[31] Ídem.

electrónica con la manuscrita, por lo que se crean una serie de mecanismos con la finalidad de protegerla. Esta protección resulta indispensable, ya que la firma digital toma tal importancia que, se podría decir que es nuestro ADN en Internet, e incluso podría ser tomada como prueba en un juicio.

Todo esto coincide con la firma de un acuerdo por parte de la ACE (Agencia de Certificación Electrónica), primera autoridad privada de certificación de España y la FESTE (Fundación para el Estudio de la Seguridad de las Telecomunicaciones) para la prestación de servicios de firma electrónica legal.

Ese acuerdo basa la prestación de certificación electrónica en la credibilidad de la fe pública de corredores de comercio y notarios, a este servicio de firma electrónica se le denomina como Certificados de Categoría 3.[32]

En España, los notarios y registradores se encuentran informados en línea, es decir, según lo dispuso la Instrucción de la Dirección General de los Registros y del Notariado del 19 de octubre de 2000, según la cual estos habrán de obtener de su corporación a una firma electrónica avanzada basada en un certificado reconocido, con un dispositivo seguro de creación de firma, al objeto de cumplir con lo dispuesto en los artículos 175 y 249 del Reglamento notarial modificado por RD 2537/1994, debiendo así los notarios solicitar información del Registro antes de autorizar las escrituras de adquisición de inmuebles, o de construcción de derechos reales sobre ellos, y posteriormente remitir el mismo día

[32] Hispasec Sistemas, Seguridad y tecnologías de la Información, Inseguridad en la firma electrónica 05/03/2000 [En línea]. Disponible: http://www.hispasec.com/, 14 abril de 2006.

del otorgamiento de las copias la comunicación de haber autorizado escritura susceptible de ser inscrita.[33]

Por último con la Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico, se regulan aspectos jurídicos de los servicios de la sociedad de la información, y de la contratación por vía electrónica, así como las obligaciones de los prestadores de servicios que actúan como intermediarios en la transmisión de contenidos por la red, la información previa y posterior a la celebración de contratos electrónicos, también las condiciones relativas a su validez, eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información. Incorporando novedades importantes como la necesidad de una constancia registral del Nombre de Dominio, ciertas obligaciones en relación con los contenidos en Internet, un régimen de responsabilidad de los prestadores de servicios de información y certificación, impulso a la elaboración y aplicación de códigos de conducta, regulación de comunicaciones comerciales y contratación por vía electrónica, solución judicial y extrajudicial de conflictos, procurando fomentar la solución extrajudicial de litigios vía arbitraje, supervisión y control infracciones y sanciones, así como reformas que permitan la informatización de los Registros Públicos.[34]

---

[33] ÁLVAREZ CIENFUEGOS, José Maria, *Instituciones del mercado financiero (contratos bancarios): Nuevas formas de contratación: banca electrónica y telefonía*, Volumen I Fuentes protección de consumidores, responsabilidad y nuevos sistemas de contratación, SOPEC Editorial S.A. Grupo Banco Santander Central Hispano, España 1999, págs. 267 y 268.

[34] Leggio, Contenidos y Aplicaciones Informáticas, S.L. Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico 11/07/2002. [En línea]. Disponible: http://www.juridicas.com/base_datos/Admin/l34-2002.html, 14 de abril de 2006.

Actualmente España trata de enfrentar la creación de una estructura sólida de certificación, mediante el uso de la firma electrónica, tratando de hacer que las empresas se familiaricen con las nuevas tecnologías al igual que la población que es la que va a darle a esta nueva tecnología la aceptación final.

Para lograr lo anterior el Consejo General de Notariado (CGN), la Agencia Notarial de Certificación (Ancert) y Microsoft Ibérica alcanzan un acuerdo para impulsar la firma electrónica, con el fin de conseguir un acuerdo de colaboración para potenciar el uso de la firma electrónica y garantizar la máxima seguridad de los sistemas de información de las notarías.

Según indica la compañía, este acuerdo será útil para potenciar la implantación de la administración electrónica en España y permitirá a las notarias ofrecer a todos los ciudadanos y a las Administraciones unos servicios más seguros y ágiles, y mejor adaptados a los requerimientos de la nueva Sociedad de la Información.

Entre los servicios que se agilizarán con su entrada en funcionamiento, Microsoft destaca la liquidación tributos por vía electrónica, la entrega de copia electrónica de escrituras a los organismos correspondiente y la obtención por vía electrónica de certificaciones catastrales, certificados de deuda de una finca o certificaciones de denominación social.

Igualmente, se procederá a la incorporación del certificado digital de Ancert al navegador Internet Explorer. De esta forma, los usuarios de certificados de firma electrónica podrán realizar trámites informáticos con la Administración Pública directamente desde el navegador de Microsoft y sin necesidad de descargarse previamente el certificado raíz de Ancert.

Además, Ancert y Microsoft colaborarán en la implantación de una plataforma basada en tecnología XML que facilite a los notarios la generación y envío de los diversos datos solicitados por las Administraciones Públicas que lo requieran. XML es un lenguaje que puede ser leído prácticamente por cualquier sistema informático, lo que facilita el intercambio de datos entre diferentes entidades y su almacenamiento de manera automática en bases de datos u otros repositorios.[35]

1.3. ESTADOS UNIDOS DE NORTE AMÉRICA

Este país cuenta con un gran número de proyectos que fueron regulando las comunicaciones hechas vía electrónica, ya que a finales de la década de los setenta, el gobierno de los Estados Unidos publicó el Data Encryption Standard (DES) para sus comunicaciones de datos sensibles pero no clasificados.

En 1993, el gobierno de EE.UU. anuncia una nueva iniciativa criptográfica encaminada a proporcionar a los civiles un alto nivel de seguridad en las comunicaciones, a ésta iniciativa se le denominó: proyecto Clipper, el cual está basado en dos elementos fundamentales:

- En un chip cifrador a prueba de cualquier tipo de análisis o manipulación el Clipper chip o EES (Escrowed Encryption Standard); y

[35] Cibernauta.com Microsoft y el Consejo General de Notariado alcanzan un acuerdo para impulsar la firma electrónica 20/12/2005, [En línea]. Disponible: http://www.elcorreodigital.com, 14 abril de 2006.

- Un sistema para compartir las calves secretas (KES- Key Escrow System) que, en determinadas circunstancias, otorgaría el acceso a la clave maestra de cada chip y que permite conocer las comunicaciones cifradas por él.

Ya desde la creación de esos proyectos y en otros que vinieron más adelante como el de estandarización del NIST the National Institute of Science Technology que introducido dentro de otro proyecto denominado Capstone el DSS Digital Signature Standard como estándar de la firma; llevo al NIST a pronunciarse a favor de la equiparación de la firma digital y la manuscrita.

Con el Tratado de Libre Comercio de América de Norte celebrado entre México, Estados Unidos y Canadá, se abre un horizonte tecnológico en cuyo contenido se contemplaban legislaciones respecto de la firma electrónica:

En su artículo 1308 dicho tratado menciona: "Las partes reconocen la importancia de las normas internacionales para la compatibilidad e interoperabilidad global de las reglas o servicios de telecomunicación y se comprometen a promover dichas normas mediante la labor de los organismos internacionales competentes tales como la Unión Internacional de Telecomunicaciones y la Organización Internacional de Normalización" [36]

México tiene una desventaja comercial respecto de Canadá y Estados Unidos (socios comerciales), comenzando por el ámbito legislativo, es decir en sus legislaciones ya se había contemplado el uso de la firma electrónica en textos legales como el de la ABA, Resolution Concerning the Cybernotary: an International Commuter Transacción Specialist del año 1994.

---

[36] DIARIO OFICIAL DE LA FEDERACIÓN, *Decreto de promulgación del Tratado de Libre Comercio de América del Norte*, publicado en el Tomo CDLXXXII, No. 14, 20 de Diciembre de 1993, p. 107.

Así que tomando como referencia el anterior régimen en años posteriores se fueron creando, textos legislativos que hicieron que E.U.A. y sus Estados que lo conforman se volvieran pioneros en el tema.

Un ejemplo de lo anterior lo encontramos en el Estado UTAH, que rebasó incluso al gobierno federal y al resto del mundo creando la primera legislación sobre firma electrónica, incluso esa ley es anterior a la ley Modelo de la UNCITRAL.

Es cuando entonces que en 1995 la Ley de firma digital del Estado de Utah: The Utah Digital Signature Act, es creada, aprobada y posteriormente modificada en 1996.

Esta Ley en su Capítulo 46-3-103 contempla definiciones como la de una firma digital estableciendo que: “Es una transformación del mensaje usando criptografía asimétrica tal, que una persona que cuente con el mensaje inicial y la llave pública de quien lo firmó, pueda determinar con precisión el mensaje en claro y si se cifró, es decir se creo usando una llave privada que corresponda a la llave pública del firmante y si el mensaje se ha alterado desde su creación”.

De lo anterior, se desprende que la firma digital es propiedad del signatario otorgándole responsabilidad en su uso, y la que no contempla algún tipo de restricción y cuyo equivalente funcional no sólo cumple con las funciones, si no que puede suplantar válidamente a una firma autógrafa, datos que el legislador mexicano puede tomar como antecedentes, sin caer en alguna copia o absoluta aplicabilidad en nuestro ordenamiento o cualquier otro que requiera las solemnidades o las formalidades en donde no tenga cabida la firma digital.

Continuando con la anterior Ley esta se encuentra dividida en cinco partes:

Parte 1 – “Título, Interpretación, Propósitos, Objetivos y Definiciones como: “autoridad de certificación con licencia”, “aceptación de un certificado”, “sistema de criptografía asimétrica”, “firma digital” y “falsificación de firma digital”.

Parte 2 - Trata sobre la concesión de licencias y la regulación de Autoridades Certificantes.

Parte 3 - Se ocupa de los deberes de la Autoridad Certificante y del contenido de los certificados.

Parte 4 – Regula los efectos de la firma digital.

Parte 5 – Se ocupa de los servicios estatales en la organización de los archivos de claves públicas y los requisitos que deben reunir.

Los objetivos de la citada ley son:

“1. Facilitar el comercio por medio de mensajes electrónicos confiables;

2. Minimizar la incidencia de falsificaciones de firmas digitales y fraudes en el comercio electrónico;

3. Establecer, en coordinación con múltiples Estados, reglas uniformes relacionadas con la autenticación y confiabilidad de los mensajes electrónicos. “

También menciona los efectos de la firma digital disponiendo que: “en donde una regla legal requiere una firma o prevé ciertas consecuencias en su ausencia, ésta regla será satisfecha por una firma digital si está verificada a una clave pública contenida en un certificado válidamente extendido por una Autoridad Certificante”.

Por lo tanto, esta ley establece la presunción de que una firma digital tiene el mismo efecto legal que una firma manuscrita si la firma digital es verificada por referencia de una clave pública incluida en un certificado válido emitido por una autoridad de certificación con licencia.

En cuanto al valor probatorio de la firma digital establece que: " El valor probatorio se basa en un criptosistema asimétrico definido como algoritmo que proporciona una pareja de claves segura".

Siguiendo con la misma ley esta también define los requisitos que debe de satisfacer una firma refiriendo que: "..... Cuando una regla de derecho requiera de una firma o requiera para ciertas consecuencias en ausencia de una firma, esa regla estará satisfecha por una firma digital sí. . . esta es verificada por la referencia de una clave pública listada en un certificado otorgado por una autoridad certificadora avanzada" otro requisito es "..... que el destinatario no tuviera conocimiento o noticia de que el signatario o ambos: ..... hayan cancelado su derecho como suscriptor o... si no se tiene legítimamente la clave privada para estampar la firma digital."

Un documento firmado digitalmente es escrito cuando: ". . . un mensaje es válido tan forzoso y efectivo como si hubiese sido escrito en papel sí: . . . la firma digital es corroborada; y . . . si la firma digital es verificada por una clave pública listada en un certificado que; haya sido expedida por una autoridad certificadora autorizada y que haya sido validada al tiempo que la firma digital haya sido creada."

En cuanto a los originales firmados digitalmente menciona: " . . . una copia de un mensaje firmado digitalmente es tan efectivo válido y forzoso como el

original del mensaje a menos que sea evidente que el signatario haya designado como único original el mensaje digitalmente firmado en cuyo caso solo ese mensaje constituirá el válido efectivo y forzoso."

En el reconocimiento legal de archivos electrónicos firmas electrónicas y contratos electrónicos hace referencia a que: " . . . un archivo o firma no podrá negársele efecto legal o cumplimiento forzoso únicamente por que se encuentra contenido en forma electrónica; así mismo . . . un contrato no podrá negársele efecto legal o cumplimiento forzoso únicamente por que un archivo electrónico fue usado para su formación; además . . . si una ley requiere un archivo electrónico en forma escrita, un archivo electrónico solventara el requisito de ley; y . . . si una ley establece una forma como requisito la firma electrónica solventara el requerimiento."

Las atribuciones y efectos de un archivo electrónico y firma electrónica los cita diciendo: ". . . un archivo electrónico o una firma electrónica es atribuible a una persona si esta fue un acto de la persona, el cuál podrá manifestarse en diversas formas incluyendo la expresión de la eficacia de cualquier procedimiento de seguridad aplicado para determinar la persona a la que el archivo electrónico o firma electrónica fue atribuida."

Habla también de la admisibilidad como prueba de la firma: "En un proceso la evidencia de una archivo o firma no podrá ser excluido únicamente por que se encuentra en forma electrónica."

Con relación a la vigencia de un certificado: " Un certificado deberá indicar la fecha en que expira, cuando esto sucede, el que suscribe y la autoridad certificadora cese de certificar la información en el certificado como se prevé en

este capítulo y la autoridad certificadora haya cumplido con sus obligaciones basadas en ese certificado" además de lo anterior establece el sistema de licencia concedida por el Departamento de Comercio de Utah, que detalla los derechos y responsabilidades de las partes de una transacción en la que se utiliza la criptografía de clave pública y una autoridad de certificación con licencia. [37]

El caso del Estado de Florida, merece especial atención, ya que éste Estado nace la ley "Florida Electronic Signature Act" de mayo de 1996 en donde reconoce el término de "International Notary" en lugar de "Cybernotary" utilizado en otras leyes de EE.UU. y propone dotar a las firmas electrónicas de la misma fuerza y efectos que las firmas manuales como ya lo previa el proyecto denominado Capstone.[38]

Así que el Comité de Seguridad de la Información de la División de Comercio Electrónico de la ABA (American Bar Association), emitió el 1 de agosto de 1996 la "Guía de firmas Digitales" (Digital Signature Guidelines), sirviendo ésta como ley de referencia de la firma digital para los legisladores de los Estados Unidos. El 15 de agosto del siguiente año en la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme, se elaboró el borrador de lo que será la "Uniform Electronic Transactions Act" la que fue aprobada el 30 de julio de 1999.[39]

---

[37] REYES KRAFFT, Alfredo Alejandro. La firma electrónica [En línea]. Disponible: http://www.razonypalabra.org.mx, 14 abril de 2006.

[38] Centro de Investigaciones en Information Technology. Firma digital Proyecto Cybernotario 20 marzo 2002 [En línea]. Disponible: http://www.it-cenit.org.ar/, 14 abril de 2006.

[39] REYES KRAFFT, Alfredo Alejandro, op cit.

Ya en 1997 el mismo Estado de Utah, redactó un proyecto de ley denominado “The Act on Electronics Notarization”.[40]

En el mismo año el Estado de California define la firma digital, como la creación por ordenador de un identificador electrónico que incluye todas las características de una firma válida, aceptable, como:

- Única y capaz de comprobarse.
- Bajo un solo control.
- Enlazándose con los datos de tal manera que sí se cambian los datos se invalide la firma.
- Adoptada al menos como un estándar en organizaciones como: The International Telecommunication Union, The American National Standards Institute, The Internet Activities Board, The National Institute of Science and Technology, The International Standards Organization

Las anteriores leyes, son bastante innovadoras al dar conceptos que se dieron a conocer al mundo y que lanzarán varias preguntas al aire, como; si ¿es necesario legislar un instrumento que apenas se conoce en Estados Unidos? y si ¿el Comercio Electrónico necesita la firma digital? Por eso se le conoce como la pionera en regular a fondo en aspectos del Comercio Electrónico y Firma Digital.

También esta ley, establece la misma presunción que en los primeros proyectos al decir que una firma digital tiene el mismo efecto legal que una firma manuscrita si se cumple que: la firma digital sea verificada por referencia a una clave pública, y que sea incluida en un certificado válido emitido por una autoridad de certificación con licencia.

---

[40] Ídem.

Conseguir que una ley que impere en la totalidad del país de los 114 millones de ínternautas, está resultando una tarea más ardua; pronosticando esto, este país se ha planteado la cuestión de determinar con un mayor grado de certeza y fidelidad la autenticación y certificación de los documentos electrónicos, especialmente con relación a otros estados que posen un adecuado régimen de seguridad de las transacciones comerciales.

Por último, el 9 de noviembre del 2001 el Congreso de los EE.UU., aprobó una legislación para sustituir la firma convencional por la digital otorgándole la misma validez legal que la materializada con tinta sobre papel, en determinados documentos.

Hoy día las consecuencias de esta ley, sin duda, serán revolucionarias, pues la firma electrónica servirá para suscribir todo tipo de contratos, hipotecas o seguros; es decir, un simple clic animará, ahora con respaldo legal, la actividad de comercio electrónico para la que se estiman transacciones de 1.9 mil millones de dólares en 2006. Con un simple clic los empresarios podrán rubricar a través del ciberespacio contratos de miles de millones de dólares, y los consumidores culminar la solicitud de una hipoteca para comprar una vivienda o un coche; además, unos y otros suscribirán seguros frente a sus pantallas.

1.4. México

Para desarrollar y entender la forma en que ha evolucionado la firma en nuestro país, explicaremos los antecedentes de ésta en cuatro etapas principales:

1.4.1. Época Precolonial

También llamada Época Indígena que comprende desde el establecimiento de los grupos aborígenes en lo que hoy es el territorio de nuestra República hasta la llegada de los conquistadores.

Cuando los primeros españoles llegaron a tierras mexicanas había una gran variedad de pueblos y razas, las que se distinguían por su civilización y avanzada organización política; Tenochtitlan, Acolhuacan (Texcoco) y Tlacopan (Tacuba) poblaciones indígenas que formaban la Triple Alianza la que sirvió de base para la expansión de México-Tenochtitlan y en consecuencia a la formación del Imperio Azteca.

No podemos asegurar que alguno de aquellos grupos o civilizaciones conocieron la firma como un medio para exteriorizar la voluntad, aún cuando algunos historiadores nos hablan, refiriéndose concretamente a la cultura Azteca, de la celebración de actos jurídicos, como la compraventa, la permuta, el arrendamiento, él deposito, entre otros, todas ellas de manera consensual.[41]

Autores como Román Piña nos hacen saber que: “Estos pueblos indígenas de México -antes de la conquista española- acostumbraban perpetuar y transmitir los hechos históricos o acontecimientos de importancia por medio de narraciones, unas veces en forma oral y otra en documentos pintados, ya fueran códices, tiras, lienzos o mapas, muchos de los cuales desaparecieron en parte

[41] ALBA H, Carlos, *Estudio comparado entre derecho azteca y derecho positivo mexicano*, Editorial Ediciones Especiales del Instituto Indigenista Interamericano, México, 1949, p.46.

debido a la naturaleza perecedera de sus materiales y en parte por su destrucción intencional."[42]

Alfonso de Zorita menciona también que tales civilizaciones "carecían de letras y por lo tanto de escritura, encontrándose todas sus antigüedades en pinturas, las cuales habían desaparecido o estaban deterioradas como consecuencia de la guerra que hicieron los españoles en contra de las deidades indígenas, y los pocos datos que se puedan recoger nos indican que los Aztecas hasta antes de la conquista desconocían casi totalmente la existencia de obligaciones procedentes de una mera manifestación de la voluntad requiriendo para la celebración de cualquier contrato, la entrega de la cosa aún cuando algunos historiadores afirman que en la venta de esclavos se necesitaba la intervención de cuatro testigos, la falta de este requisito impedía que se pudiera invocar ante algún Tribunal.[43]

1.4.2. Época Colonial

En esta etapa los españoles trasladaron a las colonias de América sus instituciones jurídicas y administrativas que en ese momento estaban vigentes en España.

Apunta Mateos Alarcón " . . . consumada la conquista impusieron en México los conquistadores, la legislación vigente entonces en España los Reyes

---

[42] PIÑA CHAN, Román, *Historia Arqueológica y Arte Prehispánico*, 1ª reimpresión, Fondo de Cultura Económica, México, 1975, p 7.
[43] ZORITA DE, Alonso, *Los señores de la Nueva España*, Editorial Imprenta Universitaria, México, 1942, p. 9.

de la nación conquistadora dictaron para los territorios americanos diversas leyes, cedulas, provisiones y ordenanzas que formaron una gran masa de derecho, las que posteriormente fueron agrupadas en un solo cuerpo de leyes que llevo el nombre de Recopilación de Indias"[44]

Los antecedentes y reglamentación legal de la firma en esta época lo encontramos en disposiciones como las Ordenanzas de Audiencias de 1530; en la Ordenanza 312 de Felipe II, en las cuales se ordenó que lo que no estuviese decidido ni declarado en las Leyes de Indias, en la Recopilación, Cédulas, Provisiones u Ordenanzas dadas y no revocadas por las Indias, se aplicaran las Leyes de Castilla y las Leyes de Toro, de igual forma en la sustancia, resolución y decisión de los cosos como en la forma y orden de sustanciar.[45]

En la Ley 114 Titulo 18 Partida 3ª, que se aplicaba supletoriamente a los súbditos de la colonia se habla de que los testigos que intervenían en ventas o permutas debían de firmar.[46]

En tanto la Ley 11 del Titulo VI, Libro II aplicada también de manera supletoria, se hablaba de que el testador firmara con su propia mano su testamento y en caso de que no supiera escribir firmaría a su ruego otra persona.[47]

---

[44] MATEOS ALARCÓN, Manuel D, *La Evolución del Derecho Civil Mexicano, desde la Independencia hasta nuestros días*, Editorial Vda. de F Díaz de León, México, 1995, p 3
[45] ZORITA DE, Alonso, *Leyes y ordenanzas reales de las Indias*, Editorial Porrua, México, 1985, p. 126.
[46] ARRAZOLA, Lorenzo, *Enciclopedia Española de derecho y Administración España y las Indias*, Tomo XI, Editorial Tipográfica General de D. Antonio Rius y Rossell, España,1999, p. 456.
[47] GUTIÉRREZ FERNÁNDEZ, Benito, *Código de estudios fundamentales de Derecho Civil Español*, Tomo II, Titulo IV, Libro II precedentes patrios fuero juzgo, Editorial Librería de Sánchez, España, 1999, p 119.

Con lo anterior podemos entender que durante la dominación española sólo las leyes que se aplicaron eran las dictadas por la península, aludiendo a la firma como un requisito meramente formal.

En la Recopilación de Indias encontramos el uso de la firma autógrafa en el testamento cerrado o escrito, del que debería realizarse en un papel cerrado con lacre, declarando el testador ante el escribano y 7 testigos que aquel papel contenía su ultima voluntad, así el escribano hacia constar la entrega y presencia de los testigos en la cubierta del testamento firmando todos los que supieran hacerlo.

De igual forma distinguían entre documentos públicos y los auténticos, por los primeros se entendía los documentos o escrituras otorgadas con las solemnidades legales ante escribano público y en la que se consigna un convenio, un testimonio u otra disposición análoga; a esos documentos las Partidas los denominan instrumentos, los cuales para que hicieran fe, se debían otorgar ante escribano, y solemnidades de los testigos y demás que prescribe el derecho

1.4.3. México Independiente

Con el movimiento insurgente que concluye con los tratados de Córdova del 27 de septiembre de 1821, hasta el Código Civil de 1870, nuestro país inicia propiamente su vida independiente y con ello un nuevo período en la legislación aunque durante la lucha insurgente y aún después de la consumación de esta, sé continuo aplicando la legislación positiva española, las Leyes de Indias y demás decretos, provisiones, reales cédulas que fueron dadas durante la Colonia.

Tales cuerpos de leyes en algunos casos resultaban inadecuados para un pueblo que se encontraba en plena formación, por lo que el gobierno provisional que asumió el poder al consumarse la Independencia, integró en noviembre de 1822 una comisión formada por los señores María Fagoaga y Andrés Quintana Roo, para elaborar un Código Civil, quienes no llegaron a cristalizar su cometido debido a la inestabilidad que existía en ese entonces en el gobierno, dado lo anterior y como ya lo mencionamos, siguieron rigiendo la vida del pueblo mexicano las mismas leyes de la Colonia hasta el día en que entro en vigor el Código Civil de 1870.[48]

El anterior Código fue el primero en promulgarse en México independiente en materia civil, el cual deroga anteriores disposiciones que junto con la ley de Partidas estuvieron vigentes.

Este cuerpo de leyes no fue lo que se dice una innovación en materia de firmas, toda vez que si tomamos en cuenta lo establecido en la Ley de Partidas, contiene una reglamentación muy similar a ella, en particular en lo que se refiere a testamentos, más sin embargo se ocupa con más precisión en la necesidad de la firma en distintos actos de la vida civil de los individuos.

Cuando este Código entró en vigor en México había sido implantada la institución del Registro Civil, por tal razón en algunos de sus artículos se hacia referencia a la firma en las actas relativas al estado civil de las personas, exigiendo en ellas la firma de los interesados, la de las autoridades políticas y la

[48] MATEOS ALARCÓN Manuel, op cit, p.5.

de los jueces encargados de llevar los libros respectivos donde se extendían las actas.[49]

También en él citado Código se menciona la firma del mandante y de los testigos; indicando igualmente cuáles son los instrumentos privados, llamando así a cualquier documento escrito por el mandante y cubierto con sólo su firma o escrito por otro y firmado por el mandante y otros dos testigos.[50]

En él mismo Código, se habla de la firma a ruego, cuando alguna de las partes en el contrato de aprendizaje no sepa hacerlo, sin embargo y a pesar de esta acertada observación no establece la forma de suplir la falta de firma en las actas del estado civil; en más artículos menciona la firma del comprador y vendedor o de otra persona a ruego cuando aquellos no sepan hacerlo; regula también la firma del testador o de quien firme a su ruego de los testigos de la firma del notario público de la firma del Juez.[51]

Por lo que respecta a la manifestación del consentimiento también establecía que esta debe de hacerse de palabra por escrito o por hechos por los que necesariamente se presuma la misma, disponiendo que, solo el que tenga imposibilidad física para hablar o escribir podrá expresar su consentimiento por otros signos indubitables.[52] Como ya lo dijimos antes los artículos anteriores no hacen mención a la imposibilidad de escribir por no saber hacerlo, ni tampoco a la forma de suplir esta incapacidad en los casos en que se exige la forma escrita.

---

[49] Ibíd. p 376.
[50] Ibíd. p 377.
[51] Ibíd. p 378.
[52] Ídem.

Así que podemos interpretar que el que no sabia escribir podría expresar su consentimiento por medio de la palabra hablada, y en los casos en que la ley exija la escritura, podrá suplir la falta de la firma por medio de la firma a ruego o de la huella digital.

En materia de testamentos, este Código, contiene disposiciones de las que podemos deducir que la firma en esta materia, es un elemento esencial para la existencia del testamento, siendo éste considerado como un acto solemne y por lo tanto, la falta de esta exigida por la ley puede considerarse que el testamento no llega a existir.

También exigía en los testamentos públicos abiertos la firma del testador, de tres testigos, la del notario y en caso de que algún testigo no supiese firmar lo hará otro de ellos por él y debiendo constar la firma entera de dos de ellos.[53] No comprendo él por que especifica que debe de ser la firma entera, sobre la base de que elementos se puede considerar así, creo que debería del limitarse a exigir la firma de dos de los testigos sin hacer la aclaración de que sea entera.

En lo que se refiere al testamento público cerrado y con relación a las a formalidades específicas, que el testador deberá de rubricar todas las hojas y firmar al calce del testamento, si no sabe o no puede hacerlo a otra persona a su ruego lo hará, esto lo especifica el artículo 3788 que enumera las formalidades legales.[54]

Como veremos más adelante la distinción entre firma y rúbrica es meramente gramatical, ya que para los efectos legales es tan válida una como la

[53] Ibíd. p 380.
[54] Ídem.

otra pero si el firmante utiliza habitualmente la firma con rúbrica deberá entenderse literalmente este precepto, no así en caso en que utilice habitualmente sólo la firma sin rúbrica o sólo la rúbrica, pues en esta situación debemos entender que deberá firmar o rubricar todas las hojas así como al calce del testamento con el fin de autenticar su contenido, en nuestro Derecho no existe como en Francia jurisprudencia al respecto.

Ya en el Código de 1884, contenía una norma de carácter general relativa a la formalidad que debían sujetarse los actos jurídicos; dicha disposición se establece que cuando una persona no sepa escribir firmara por ella otra persona a su ruego ante dos testigos.[55]

El citado código nos señala que es lo que debe entenderse como instrumento privado estableciendo que es él instrumento otorgado por el mandante, pero esa definición se puede hacer extensivo, es decir que el legislador de aquella época extendió por los instrumentos privados cualquier documento escrito y cubierto sólo con la firma del otorgante o escrito por otro y firmado por el otorgante y dos testigos.[56]

Del estudio de las anteriores disposiciones que estuvieron vigentes en México desde el 15 de septiembre de 1810 hasta el 30 de septiembre de 1932, se llega a la conclusión de asegurar que en la celebración de los diversos actos jurídicos realizados en forma escrita, las personas que en ellos intervinieron usaron la firma como medio de exteriorizar su voluntad para adquirir derechos obligaciones o para dar autenticidad a los actos.

---

[55] Ibíd. págs 381 y 382.
[56] Ídem.

Por lo que respecta a su reglamentación existía una forma indirecta; esto es no encontramos en las invocadas leyes, ningún capítulo sobre la firma en particular.

En resumen, en las legislaciones civiles de 1870 y 1884 se reconoce una reglamentación de la firma la cuál existe en forma indirecta pues no encontramos disposición legal o capítulo alguno que reglamente la firma en particular, sin bien se concluye que era una persona al celebrar actos jurídicos en forma escrita, otorga su firma en el documento como medio de exteriorizar su voluntad para adquirir derechos y obligaciones o para autenticar. Cabe mencionar que el Código Civil de 1884 tuvo vigencia hasta el 30 de septiembre de 1932.

Así que los principales antecedentes legislativos en materia de firma y certificación digital en nuestro país se encuentran en el Código de Comercio de 1884, en el que existen disposiciones relativas al telégrafo como medio de comunicación; en el Código Civil de 1928 se hace referencia en diversas disposiciones al teléfono; en el Código de 1932 donde por cierto se omite expresar los elementos que debe de contener la firma; pero sí menciona la obligación de imprimir la firma, impuesta a todos los que intervenían en actos jurídicos; menciona también que debía estamparse la firma entera.

Esto último género un punto de discusión entre legisladores de aquel tiempo ya que consideraron que existe una gran laguna al mencionar el término de firma entera; dado que se tendría que determinar si una firma incompleta es válida o no, éste término viene en copia textual desde el código de 1870 pasando así por el de 1884 disposiciones que en su mayoría fueron trasladadas textualmente al Código de 1932 inclusive con las mismas lagunas y defectos de que adolecían.

Por último, mencionemos a las leyes bancarias de 1990 que incorporan a los medios telemáticos; ya en tiempos más actuales la Ley de Protección al consumidor de 1992 que protege a los consumidores de las ventas a distancia y telemarketing, es decir ventas por medios de comunicación masiva como el radio y televisión; dentro de diversas Leyes Fiscales de 1998 igualmente se prevén declaraciones y pagos en formato electrónico, además de diversos esfuerzos gubernamentales; pero las anteriores legislaciones las estudiaremos más a fondo en posteriores capítulos.

1.5 LATINOAMÉRICA

1.5.1 Argentina

En este país desde 1998 por Decreto No. 427/98 se reguló el uso de la firma digital para actos internos del Sector Público, este Decreto tenía como objetivo optimizar la actividad de la administración pública adecuando sus sistemas de registro de datos, los que iban tendientes a eliminar el uso del papel; así mismo este Decreto da definiciones como el de firma digital, documento digital firmado; indica que la supervisión y control de los métodos digitales estarán a cargo de la Secretaria de la Función Pública, la cuál regulará la actividad de las instancias que intervienen en la emisión de certificados tales como las autoridades certificantes y organismos auditantes, que son los encargados de la protección de datos y de dar elementos de seguridad necesarios para ese fin.

Es importante mencionar que a la firma digital le da el mismo efecto y valor que el de una firma ológrafa.

En marzo de 1999 un grupo de juristas que integraban una Comisión establecida por Decreto número 685/95, se encargó de la redacción de un Proyecto de Código Civil que abarcase las materias electrónicas y comerciales, manteniendo la regla de libertad de formas pero conservando la forma convenida que es obligatoria para las partes bajo pena de invalidez del negocio jurídico.

Algo de lo más relevante que contempla tal proyecto es que:

a) Sé amplia la noción de escrito, de modo que se puede considerar expresión escrita la que se produce, consta o lee a través de medios electrónicos.

b) Define a la firma y considera satisfecho el requisito de la misma cuando en los documentos electrónicos se sigue un método que asegure razonablemente la autoría e inalterabilidad del documento.

c) Prevé la posibilidad de que existan instrumentos públicos digitales.

d) En las escrituras públicas se incorporan primero la justificación de la identidad, que sustituye a la fe de conocimiento, previniendo incluso la posibilidad de insertar la impresión digital del compareciente no conocido por el notario; y segundo la reglamentación de las actas, a las que sólo se les asigna valor probatorio cuando son protocolares.

e) En materia de instrumentos privados regula el valor probatorio del documento electrónico que se vincula a usos y a las relaciones preexistentes de

las partes y a la confiabilidad de los métodos usados para asegurar la inalterabilidad del texto.[57]

En diciembre del 2001 se publicaron en el Boletín Oficial de la Ley No. 25.506 de Firma Digital Argentina que tiene por objeto reconocer el empleo de la firma tanto electrónica como digital.

Para dicha ley la firma digital es: "el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose este, bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración en el documento digital posterior a su firma"[58]

De la anterior definición se derivan los principios de identidad inalterabilidad y certificación lo que representa un gran acierto para dicha legislación que también requiere para considerar como válida dicha firma, el ser creada durante el período de vigencia del certificado digital, verificada por las autoridades correspondientes y por un certificador, por ende la firma electrónica la define como aquella que carezca de alguno de los requisitos legales para ser digital.

El artículo 5 de dicha ley establece: "se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de

---

[57] CÓDIGO CIVIL ARGENTINO, ANOTADO Y CONCORDADO, Editorial Claridad, Argentina, 1999, p 170.

[58] Subsecretaria de la Gestión Publica, Jefatura de Gabinete de Ministros. República de Argentina Infraestructura de Firma Digital de la República Argentina 5 enero de 2006 [En línea]. Disponible: http://www.pki.gov.ar/ 25 marzo de 2006.

identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez" [59]

Esta ley cumple con los estándares internacionales y prevé disposiciones avanzadas como lo establecido el artículo 4to, que establece excepciones a la aplicación de dicha ley como la causa de muerte, derecho de familia, actos personalísimos y los actos que contengan exigencias o formalidades incompatibles como la utilización de la firma digital.

De dichas excepciones se puede desprender que el legislador argentino pone especial atención a que si bien mundialmente las legislaciones de Norteamérica representan la mayor innovación en términos tecnológicos, dichas disposiciones no pueden tener aplicación exacta en ordenamientos distintos al Common Law debido a que la forma y sus consecuencias son aspectos que del todo son distintos entre ambos ordenamientos.

Por lo que respecta a los certificados digitales, éstos deben ser emitidos por un certificador avalado por la Subsecretaria de Gestión Pública debiendo de tener un formato que permita el reconocer a su titular, al certificador y el tipo de política de certificación empleada, dichos cerificados solo podrán expedirse por el gobierno, es decir ningún particular puede elaborar un certificado.

El Código Civil Argentino es uno de los ordenamientos que contiene más disposiciones legales acerca de la firma, hay que reconocer que este establece una normativa estricta previendo como una condición para la existencia de un acto jurídico bajo la forma privada el otorgamiento de la firma de las partes,

[59] Ídem.

ya que la omisión de esto quita valor al instrumento pero al disponer que signos e iniciales no valen como firma, tampoco considera como firma el hecho de que una persona haga la escritura de su nombre y apellidos salvo que así lo acostumbre suscribir todos los actos de su vida pública y privada y que esta manera peculiar de firma sea reconocida según se desprende de lo que dice el su artículo 1014 que establece: "ninguna persona puede ser obligada a reconocer un instrumento que este solo firmado por iniciales o signos, pero si el que lo hubiere firmado lo reconociera voluntariamente, las iniciales o signos valen como la verdadera firma"[60]

Lo que interpretado a contrario sensu, nos hace pensar que el Código Civil Argentino abre las puertas a que una persona pueda tener más de una firma.

El mismo Código contiene disposiciones acerca de la firma en blanco, la firma en los testamentos, fechas o días en que se puede otorgar la firma, la firma ruego, el reconocimiento judicial de la firma, cotejo y comparaciones de la firma en caso de duda o de posibles falsificaciones.

Por último, esta legislación carece de algunos elementos de claridad, certeza y seguridad jurídica sugeridos por la CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional), un ejemplo de esto es que la legislación Argentina contiene normas que exigen para la prueba de los negocios, el doble ejemplar, la firma y fecha cierta aunque en realidad acepta el nacimiento de obligaciones aunque no se observen estos requisitos como en la transferencia electrónica de fondos; pero también es de destacar que es una de las primeras en contener un capítulo especifico al respecto.

---

[60] CÓDIGO CIVIL ARGENTINO, ANOTADO Y CONCORDADO, op cit, p 35-40.

1.5.2. Chile

En este país en 1998 se creó la Comisión Nacional para las Nuevas Tecnologías de información y Comunicación, en calidad de órgano asesor del Presidente de la República de Chile y bajo la dirección del Ministro de Economía Fomento y Reconstrucción, cuya misión principal fue elaborar una visión prospectiva sobre las tendencias e impactos del desarrollo de las tecnologías de información y comunicaciones, además de elaborar una propuesta con lineamientos estratégicos y acciones concretas para potenciar la difusión de nuevas tecnologías así que platea la necesidad de iniciar el desarrollo de un marco jurídico que valide el uso del documento y firmas digitales tanto para el Estado como para el desarrollo del comercio electrónico.

Así que en el año de 1999 el entonces presidente de Chile, Eduardo Frei presentó el Decreto número 81/99 del 10 de junio de 1999 publicado el 26 del mismo mes y año, el que regula el uso de la firma digital y los documentos electrónicos o digitales en la Administración del Estado, este Decreto tiene como objetivo regular la utilización de la firma digital y los documentos electrónicos como un soporte alternativo a la instrumentalización en papel de las actuaciones de los órganos estatales dotándolos del marco legal que permita el uso de la informática en reemplazo de los procedimientos manuales.

Este Decreto hace mención de algunas definiciones como:

a) Firma electrónica: Código informático que permite determinar la autenticidad de un documento electrónico y su integridad, impidiendo a su trasmisor desconocer la autoría del mensaje en forma posterior;

b) Firma digital: Especie de firma electrónica que resulta de un proceso informático validado e implementado a través de un sistema criptográfico de claves públicas y privadas;

c) Documento electrónico: Toda representación informática que da testimonio de un hecho;

d) Clave privada: Aquella que solo es conocida por el titular del par de claves y que es usada para añadir una firma digital a un documento electrónico o para desencriptar un documento electrónico previamente encriptado por medio de la correspondiente clave pública;

e) Clave pública: La que es empleada para verificar la firma digital añadida a un documento electrónico por el titular o para encriptar documentos destinados a ser transmitidos a él.

En cuanto al valor probatorio de los documentos escritos en un soporte electrónico éstos producirán los mismos efectos que los escritos en un soporte de papel, en los primeros documentos la firma digital sustituirá a la firma ológrafa del funcionario que lo emite y producirá los mismos efectos que aquella.

Así la firma digital sustituirá el uso de sellos, timbres, visto bueno u otra marca distinta que fuere necesaria para la validez del documento si este hubiere sido escrito sobre un soporte de papel.

También debemos señalar que dicho Decreto no hace referencia a las instancias que intervienen en la emisión de certificados ni tampoco algo especifico

en cuanto a la protección de datos ni mucho menos a la responsabilidad por daños y perjuicios o sanciones derivados de su uso.[61]

En el 2000 se elabora un proyecto de ley que regula la firma electrónica, la prestación de servicios de certificación y el procedimiento voluntario de acreditación de prestadores de servicios de certificación para su uso en actos o contratos celebrados por medio de documentos electrónicos a través de medios electrónicos de comunicación. Este proyecto es el antecedente de la Ley del mismo nombre que fue promulgada y entró en vigor en el 2002.

La cual más adelante resultaría igual de controvertida que la Ley Argentina, por no apegarse a la Ley Modelo de la CNUDMI, y la que además crea sus propios conceptos, como los siguientes:

a) Firma digital avanzada: " aquella certificada por un prestador acreditado que ha sido creada usando medios que el titular mantiene bajo su exclusivo control de manera que se vincule únicamente al mismo y a los datos a que se refiere, únicamente permitiendo la detección posterior de cualquier modificación verificando la identidad del titular e impidiendo que se desconozca la integridad del documento y su autoría".

Los efectos jurídicos de esta Ley recaen en los actos y contratos otorgados o celebrados por personas naturales o jurídicas suscritos por medio de firma electrónica, los que serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escritos y en soporte de papel.

---

[61] FERNÁNDEZ DELPECH, Horacio, Trabajo preparado por un grupo de alumnos de la Cátedra Marco Legal a cargo del Dr. Horacio Fernández Delpech, del Master año 2004 en Dirección de Empresas dictado por USAL (Argentina) - Universidad de Deusto (España) Alumnos autores: Carlos Fernando Barberán, et. al, Firma Digital [En línea]. Disponible: http://www.hfernandezdelpech.com.ar/, 14 abril de 2006.

Del punto anterior, se excluye a aquellos en que la ley solicite una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, en los actos que la ley requiera de la concurrencia personal de alguna de las partes y aquellos actos relativos al derecho de familia.

b) Firma electrónica: “cualquier sonido símbolo o proceso electrónico que permite al receptor de un documento electrónico identificar al menos formalmente a su autor”.

Se tomará como firma manuscrita para todos los efectos legales, y los documentos electrónicos que tengan la calidad de instrumento público deberán suscribirse mediante firma electrónica avanzada.

c) Documento electrónico: “ Toda representación de un hecho o imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior”.

En relación con los documentos electrónicos éstos podrán presentarse en juicio y harán prueba plena de acuerdo con las reglas generales, y los que tengan la calidad de instrumento privado tendrán el mismo valor probatorio en cuanto hayan sido suscritos mediante firma electrónica avanzada.

d) Certificado de firma electrónica: “Certificación electrónica que da fe sobre los datos referidos a una firma electrónica simple o avanzada.

e) Certificador: entidad prestadora de servicios de certificación de firmas electrónicas”.

En lo que respecta a la certificación de la firma, se da entrada a personas públicas y privadas con el único requisito de obedecer las reglas prácticas de

certificación, manteniendo un registro de acceso público a los certificados en donde se hace constar los emitidos y los que quedan sin efecto.

Así también, los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por los prestadores establecidos en el país, bajo su responsabilidad y cumpliendo los requisitos fijados en la ley y su reglamento.

f) Usuario o titular: "Persona que utiliza bajo su exclusivo control un certificado de firma electrónica". [62]

Los usuarios de los certificados están obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador.

1.5.3. Colombia

En este país no es mucha la legislación en materia de comercio electrónico o implementación de firma digital, algunas de las leyes existentes han sido elaboradas sobre la base de la Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

La anterior Ley Modelo sirvió de base a la Ley 527/99 sobre Mensajes de Datos, Comercio Electrónico y Firma Digital, del 18 de Agosto de 1999, cuyo objetivo es definir y reglamentar el acceso al uso de mensajes de datos del comercio electrónico y de las firmas digitales, estableciendo las entidades de

[62] CUERVO ÁLVAREZ, José. La firma digital y entidades de certificación 1998-2002 [En línea]. Disponible: http://www.informatica-juridica.com/, 14 abril de 2006.

certificación, y su ámbito de aplicación que según su artículo 1º dice: "La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos"; y más adelante entre otos conceptos define:

- Mensaje de datos: Información generada, enviada, recibida, almacenada o comunicada por medios electrónicos ópticos o similares como pudieran ser entre otros el intercambio Electrónico de Datos (EDI) Internet, el correo electrónico, el telegrama el telex o telefax;[63]

Acerca del mensaje de datos esta misma Ley 527/99 en su artículo 10 establece que los mensajes de datos serán admisibles como medios de prueba teniendo la misma fuerza probatoria otorgada a los documentos en papel, ya prevista en el Código de Procedimientos Civil Colombiano en su CAPÍTULO VII del Titulo XIII, el que describe las distintas clases de documentos públicos y privados así como a la exhibición de estos.[64]

---

[63] ITEnLinea Administración Estratégica del Recurso Informático. Importancia de la firma digital Por: Wilson Barón, Director de Operaciones para la Región Andina de Afina 16 septiembre 2005 [En línea]. Disponible: http://www.itenlinea.com/, 14 abril de 2006.

[64] El Código de Procedimiento Civil Colombiano en su artículo 251 en lo que se refiere a los instrumentos públicos y privados la principal consecuencia de la distinción radica en que tratándose de públicos son otorgados por funcionarios públicos en ejercicio de su cargo o con su intervención, resaltando que cuando consiste en un escrito autorizado o suscrito por el respectivo funcionario, es instrumento público; cuando es otorgado por Notario y fue incorporado a su respectivo protocolo, se denomina escritura pública; reuniendo así la característica de mayor seguridad, autenticidad, e integridad otorgándoles el derecho el máximo valor probatorio. Y en su artículo 254 tratándose de copias el mismo Código señala que tendrá el mismo valor probatorio del original en los siguientes casos: cuando hayan sido autorizadas por Notario, Director de Oficina Administrativa o de Policía, previa orden del Juez donde se encuentre el original o una copia autenticada; cuando sean autenticadas por Notario, previo cotejo con el original o la copia autenticada que se le presente y cuando sean compulsadas, del original o de copia autenticada en el curso de inspección judicial, salvo que la ley disponga otra cosa. Senado de la República de Colombia, Información legislativa Leyes desde 1992 - Vigencia Expresa y Sentencias de Constitucionalidad, 9 de marzo de 2006. [En línea]. Disponible: http://www.secretariasenado.gov.co/, 14 abril de 2006.

Continuando con esta misma Ley también define:

"- Firma digital: Valor numérico que se adhiere a un mensaje de datos y que utilizando un procedimiento matemático conocido vinculado a la clave del indicador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del indicador y que el mensaje inicial no ha sido modificado después de efectuada la transacción;

- Entidad de certificación: Persona autorizada conforme a la ley que esta facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas las comunicaciones basadas en las firmas digitales". [65]

La anterior definición se liga a las funciones de supervisión y control de certificación la cual es considerada como: "una función pública a cargo de, cámaras de comercio, personas morales públicas y privadas que estén autorizadas por la Superintendencia de Industria y Comercio", que entre otras funciones que veremos más adelante es la encargada de imponer sanciones a las entidades de certificación, ya que dentro de sus obligaciones se encuentra la de llevar un registro de los certificados, garantizando la protección, confidencialidad y debido uso de la información suministrada por el suscriptor, el que también es responsable por falsedad, error u omisión en la información proporcionada a la entidad de certificación.

Igualmente esta Ley limita la autorización a las Autoridades de Certificación sólo a personas jurídicas, ya que si bien es más fácil controlar sus

[65] ITEnLinea Administración Estratégica del Recurso Informático, op cit.

actividades, también es cierto que existen profesionales que no laboran dentro de una persona moral y bien pueden fungir como Autoridades de Certificación, como lo son los notarios públicos o corredores.

En cuanto a los elementos de seguridad, esta Ley indica que la información consignada en un mensaje de datos será integra, si esta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

Con relación al valor probatorio de una firma digital, establece que esta tendrá la misma fuerza y efectos que el uso de una firma manuscrita, sólo si la digital incorpora los siguientes atributos:

- " Es única a la persona que la usa
- Es susceptible de ser verificada
- Esta bajo control de la persona que la usa y
- Ligada a la información o mensaje de tal forma que si se cambia el contenido de la firma ésta no será válida".[66]

De acuerdo a lo anterior, en este país se puede celebrar cualquier tipo de acto jurídico mediante la firma digital siempre y cuando reúna los requisitos antes señalados, uno puede tanto reconocer un hijo o acudir ante la autoridad judicial en una diligencia de carácter personal, ya que no existe limitante expresa en dicho ordenamiento, lo cuál es contrario a la Ley Modelo de la UNCITRAL, y por lo tanto es entonces es más parecida a la legislación estadounidense en donde las restricciones para su uso son muy ilimitadas.

---

[66] Ídem.

El 2000 es un año muy importante con relación a las entidades de certificación, los certificados y firmas digitales, ya que el 11 de septiembre con el Decreto 1747, que es reglamentario de la Ley 527/99 se refiere a las entidades de certificación, los certificados y las firmas digitales estableció en sus primeros artículos las demás definiciones para efectos de ese decreto, señalando que es un iniciador, un suscriptor, calve privada, clave pública, certificado en relación con firmas digitales, estampado cronológico, entidad de certificación cerrada y abierta.

Así que las entidades de certificación de dividen en 2 clases: las abiertas y las cerradas y como control supremo de ambas la Superintendencia de Industria y Comercio, lo cuál dará mayor credibilidad a los documentos electrónicos emitidos por sus diferentes entidades al darle validez a la firma electrónica.[67]

También es de mencionarse que la Corte Constitucional de Colombia en su sentencia del 8 de junio del 2000, se refirió a la necesidad de actualizar los

[67] La Corte Constitucional de Colombia en su sentencia del 8 de junio de 2000 y con motivo de que algunos ciudadanos instauraran acción pública de inconstitucionalidad en contra de la Ley 527, por considerar que la fe pública es un acto que otorga exclusivamente el Estado a través de sus Notarios Públicos y no las entidades particulares como lo son las Cámaras de Comercio, finalmente la Corte en la anterior sentencia declaro constitucional en su totalidad la Ley, resaltando aspectos importantes como la posibilidad de que un ente público o privado con poderes de certificar proporcione seguridad jurídica a las relaciones comerciales por vía informática, que estos entes son las entidades de certificación que una vez autorizadas están facultados para emitir certificados en relación con las claves de todas la personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir con las funciones relativas las comunicaciones basadas en firmas digitales. Considera que la naturaleza de la función de las entidades de certificación es un servicio público pero según él artículo 365 de la Constitución de ese país los servicios públicos pueden ser prestados por entidades públicas o privadas o conjuntamente. Le permite que el servicio lo presten particulares siempre y cuando reúnan los requisitos exigidos por ley y cuenta con la aprobación de la Superintendencia, organismo rector para todos los efectos. DÍAZ GARCÍA, Alexander, REDI Revista Electrónica de Derecho Informático, Los Documentos Electrónicos y sus Efectos Legales en Colombia, Numero 34, Mayo 2001 [En línea]. Disponible: http://premium.vlex.com/doctrina/REDI, 14 abril de 2006.

regímenes jurídicos, para otorgar fundamento jurídico al intercambio electrónico de datos, agregando que el propósito de la promulgación de nuevas normas, es el de actualizar la legislación nacional y ponerla a tono con las nuevas realidades de comunicación para darle fundamento jurídico, no solo a las transacciones comerciales si no también fuerza probatoria a los mensajes de datos. Igualmente más adelante declara que: el mensaje de datos como tal debe de recibir el mismo tratamiento de los documentos consignados en papel, es decir deber dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento.[68]

1.5.4. VENEZUELA

A partir de 1997 empiezan a desarrollarse algunas iniciativas relacionadas con la economía en red, en particular de comercio electrónico y sólo a partir de 1999, se puede decir que se dío inicio al proceso de desarrollo de la economía en red.

El desarrollo de un gobierno electrónico en Venezuela se encuentra en una fase de inicio muy preliminar, y al igual que en otros países de Latinoamérica se requieren de grandes inversiones para llegar a los niveles adecuados.

En la actualidad el marco regulatorio del sector de Tecnologías de Información y Comunicaciones (TIC) en este país es muy diverso, como la nueva Ley Orgánica de Telecomunicaciones y los reglamentos derivados de la misma (por ejemplo Lineamientos de la Apertura, Interconexión y Plan de Numeración), el

[68] Ídem.

Decreto 825 mediante el cual se declara el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de Venezuela. [69]

El Decreto No 1.204 que tiene el rango y fuerza de Ley que trata sobre Mensajes de Datos y Firma Electrónica, el cual fue aprobado por el Congreso Venezolano, y publicado en la Gaceta Oficial No 37 del 28 de febrero del 2001, en su artículo 1º establece que el objetivo de este Decreto-Ley es: ".... otorgar y reconocer la eficacia y valor jurídico a la firma, al mensaje de datos y a toda la información inteligible en formato electrónico, independientemente de su soporte material atribuible a personas naturales o jurídicas públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y los certificados electrónicos". También menciona que su ámbito de aplicación o cobertura son: ".... los mensajes de datos y firmas electrónicas independientemente de sus características tecnológicas de los desarrollos tecnológicos que se produzcan en un futuro". [70]

En su artículo 2º menciona entre otros conceptos, que para efectos del Decreto-Ley se entenderá por:

- "Persona: sujeto jurídicamente hábil bien sea natural, jurídica, pública, privado nacional o extranjera susceptible de adquirir derechos y contraer obligaciones.

---

[69] Gobierno Bolivariano de Venezuela, Ministerio de Ciencia y Tecnología, Centro Nacional de Tecnologías de la Información, Directorio de Gobierno Electrónico Venezuela, Decreto 825, 10 mayo 2000. [En línea] Disponible: http://www.gobiernoenlinea.gob.ve/directorioestado/decreto_825.html , 14 abril de 2006.

[70] Ídem.

- Mensaje de datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

- Emisor: Persona que origina un mensaje de datos por sí mismo o través de terceros autorizados.

- Signatario: Es la persona titular de una firma electrónica o certificado electrónico.

- Destinatario: Persona a quien va dirigido el mensaje de datos.

- Proveedor de servicios de certificación: Persona dedicada a proporcionar certificados electrónicos y demás actividades previstas en este Decreto-Ley

- Acreditación: Título que otorga la Superintendencia de Servicios de Certificación Electrónica a los proveedores de servicios de certificación para proporcionar certificados electrónicos una vez cumplidos los requisitos y condiciones establecidas en este Decreto.

- Certificado electrónico: Mensaje de datos proporcionado por un proveedor de servicio de certificación que le atribuye certeza y validez a la firma electrónica.

- Firma electrónica: Información creada o utilizada por el signatario, asociada a un mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado". [71]

Para que dicha Firma Electrónica vincule al signatario con el mensaje de datos y se atribuya la autoría de este, tendrá la misma validez y eficacia probatoria que la ley otorga a la Firma Autógrafa si reúne los requisitos señalados en el artículo 16 del mismo Decreto-Ley:

---

[71] Ídem.

- “Garantía de que los datos usados para su generación puedan producirse solo una vez y asegurar razonablemente su confidencialidad.

- Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en el momento.

- No alterar la integridad del mensaje de datos.

- La firma electrónica podrá formar parte integrante del Mensaje de Datos, o estar inequívocamente asociada a este; enviarse o no en un mismo acto”. [72]

En este último punto me parece que tendrían que haber tomado como ejemplo otras legislaciones ya que una firma digital debe necesariamente estar contenida en el mismo texto electrónico del mensaje de datos que se envía, de lo contrario un día se redacta un contrato, mañana lo envió por correo electrónico y pasado lo firmo, teniendo la misma validez y eficacia probatoria que una firma autógrafa, lo que otorgaría mayor certeza jurídica si todo se realizara en un solo acto.

Por otro lado en lo que respecta a la solemnidad y a las formalidades, dicho ordenamiento en su artículo 6º establece: “Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, estas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto-Ley” Y continua diciendo “Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, este requisito quedara satisfecho en relación con un Mensaje de datos al tener asociado una Firma Electrónica”. [73]

---

[72] Ídem.
[73] Ídem.

De acuerdo a lo anterior no solo cualquier acto puede celebrase mediante una Firma Electrónica, sino que cuando la Ley requiera de una Firma Autógrafa, esta puede ser reemplazada por una Electrónica, argumentos que tendríamos que considerar cuando realmente se requiera de una Firma Autógrafa para la celebración o validez de determinados actos.

Por lo que hace a la supervisión y control, esta se encuentra a cargo de la Superintendencia de Servicios de Certificación Electrónica que depende del Ministerio de Ciencia y Tecnología, esta Superintendencia también podrá adoptar las medidas preventivas o correctivas necesarias para que se garantice la confiabilidad de los servicios prestados por los proveedores de servicios de certificación, uso de estándares o prácticas internacionalmente aceptadas o que el proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad o el buen uso del servicio. Los proveedores de servicios de certificación tienen la obligación de garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione como mantener un respaldo confiable y seguro de dicha información, garantizar la adopción de las medidas necesaria para evitar la falsificación de certificados electrónicos y de las firmas electrónicas que proporcionen.

Aunado a lo anterior la protección de los mensajes de datos estarán sometidos a las disposiciones constitucionales y legales que garanticen los derechos a la privacidad de las comunicaciones y de acceso a la información personal.

También reconoce los Certificados Extranjeros al decir que estos certificados electrónicos emitidos por proveedores de servicios de certificación

extranjeros tendrán la misma validez y eficacia jurídica reconocida en el Decreto-Ley siempre que sean garantizados por un proveedor de servicios de certificación debidamente acreditado, que garantice en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos de seguridad, válidez y vigencia de un certificado, si un certificado extranjero no cumple con lo antes mencionado, este carecerá de efectos jurídicos.

Por último en cuanto a las responsabilidades por daños y prejuicios y las sanciones este Decreto-Ley es claro al mencionar las obligaciones del signatario, como es la de actuar con diligencia para evitar el uso no autorizado de su firma electrónica y notificar a su proveedor de servicios de certificación que su firma electrónica ha sido controlada por terceros no autorizados o indebidamente usada cuando tenga conocimiento de ello; si el signatario no cumple con las obligaciones antes referidas será responsable de las consecuencias del uso no autorizado de su firma electrónica. [74]

1.6. ORGANISMOS INTERNACIONALES

1.6.1 UNCITRAL-CNUDMI

La legislación derivada de los trabajos de la UNCITRAL (United Nations Comisión for the International Trade Law) también conocida por sus siglas en español CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional), se ve reflejada en la elaboración de Leyes Modelos, además de la

[74] Ídem.

preparación de convenciones y tratados internacionales; las Leyes Modelos constituyen una técnica indirecta de uniformidad ya que estas carecen de valor normativo por que su texto tiene el valor de un mero ejemplo orientativo destinado a los legisladores nacionales con la recomendación de que la opten como un modelo al dictar leyes internas en la materia. [75]

Es precisamente la UNCITRAL el primer órgano internacional que elabora Leyes Modelo en materia de comercio electrónico y en materia de intercambio electrónico de datos (EDI), el antecedente de este organismo lo encontramos en la Recomendación de 1985 la que sugería a los países miembros de la ONU, que modificaran sus sistemas legislativos; en especial con aquellas normas que tengan que ver con la aceptación de pruebas basadas en sistemas informáticos, con la exigencia de que determinados actos se hagan de manera escrita, ampliando este concepto a la informática; sobre la misma línea examinará la firma manuscrita para aceptar la firma o autenticación a través de medios electrónicos.

Así, en un principio no había mucha respuesta de los países miembros de las Naciones Unidas, a pesar de que se siguieron haciendo propuestas para cambiar algunos principios jurídicos aplicables a la formación de contratos mercantiles internacionales por medios electrónicos.

No fue hasta que en 1996 el 16 de diciembre mediante Resolución General de la Asamblea 51/162, que se contempla la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional y que regula principalmente al Comercio Electrónico, tiene como principales objetivos:

---

[75] PÉREZ NIETO CASTRO, Leonel, *Derecho Internacional Privado*, Editorial Oxford University Press, Séptima edición, México, 2002, p. 40.

- “Garantizar la seguridad jurídica en el contexto del uso más amplio posible del procesamiento automático de datos en el comercio internacional.

- Ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional con lo que se pueden eliminar algunos de los obstáculos jurídicos creando un marco jurídico para un desarrollo más seguro de las vías electrónicas de negociación es decir el comercio electrónico.

- Facilitar y fomentar el uso y crecimientos del comercio electrónico a escala internacional y que sea aceptable por los Estados con sistemas jurídicos sociales y económicos diferentes para que a través de la estandarización de normas relativas a este tipo de comercio, se contribuya a establecer relaciones económicas internacionales armónicas y unificadas.

- Facilitar el empleo del comercio electrónico, concediendo igualdad de trato a usuarios de mensajes consignados sobre soporte informático que los usuarios de la documentación consignada sobre papel”.

Su ámbito de aplicación será a todo tipo de información en forma de mensajes de datos empleada en el contexto de actividades comerciales; que abarca desde el uso de la tecnología de redes cerrada (EDI) y tecnología de redes abiertas (Internet y correo electrónico), además busca que sea aplicable en un futuro a cualquier tecnología que llegare a existir.

Esta Ley Modelo esta dividida en dos partes, la primera parte regula el comercio electrónico en general, y la segunda parte regula el uso del comercio electrónico en determinadas ramas de la actividad comercial.

La primera parte a su vez consta de tres capítulos el primero de ellos trata las disposiciones generales, el segundo la aplicación de los requisitos jurídicos a

los mensajes de datos y el tercero se refiere a la comunicación de los mensajes de datos.

En esta primera parte el artículo 7º recoge el concepto de firma el que regula el equivalente funcional de firma estableciendo los requisitos de admisibilidad de una firma producida por medios electrónicos, que nos da un concepto amplio de firma electrónica indicando: "Cuando la ley requiera la firma de una persona ese requisito quedara satisfecho en relación con un mensaje de datos":

"a) si se usa un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) si ese método es tan fiable como sea apropiado para los fines para los que se creó o comunico el mensaje de datos a la luz de todas las circunstancias del caso incluido cualquier acto pertinente. [76]

Sobre los capítulos segundo y tercero de esta primera parte de la Ley Modelo, cabe mencionar que el segundo expresa el mínimo aceptable en materia de requisitos de forma para el comercio electrónico por lo que deberán ser tenidas por imperativas, salvo que en ellas mismas de disponga lo contrario, es aclarar que el hecho de considerar como mínimo aceptable a dichos elementos, no es una invitación a establecer requisitos más estrictos que los enunciados en la Ley Modelo; y la tercera parte esta construido sobre el principio de la autonomía de la voluntad de las partes es decir supone una sugerencia a los contratantes, misma que puede ser modificada, previo acuerdo de las partes, que así mismo puede servir de punto de partida a los interesados en contratar a través de estos

[76] FERNÁNDEZ DELPECH, Horacio, op cit.

medios, estas normas fijan una conducta mínima para el intercambio de mensajes de datos en casos en los que no se haya concretado acuerdo alguno para el intercambio de comunicaciones entre las partes.

El 12 de diciembre de 2001 fue aprobada la Ley Modelo sobre Firma Electrónica, por el Grupo de Trabajo de la CNUMDI sobre Comercio Electrónico reunido del 18 al 29 de septiembre de 2000 en Viena, de tal reunión se establecieron los objetivos siguientes:

- Reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del uso de técnicas modernas a las que puedan denominarse en general firmas electrónicas.

- Establecer normas básicas para la armonía jurídica y la interoperabilidad técnica.

- Mejorar el entendimiento de las firmas electrónicas y la seguridad de que puede confiarse en determinados técnicas de creación de firma electrónica en operaciones de importancia jurídica.

- Crear normas practicas para comprobar la fiabilidad técnica y la eficacia jurídica que cabe esperar de una determinada firma electrónica.

- Establece un principio de no-discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente, así como las técnicas que pueden utilizarse para comunicar o archivar electrónicamente información.

Esta ley será aplicable en todos los casos en que se utilice en firmas electrónicas en el contexto de actividades comerciales. (Artículo 1º).

Algunas de las definiciones que contempla dicha Ley Modelo se encuentran contenidas en el artículo 2º, que entre otras define a un certificado, mensaje de datos, firmante, prestador de servicios de certificación, etc., también puntualiza que por firma electrónica se entenderán: los datos en forma electrónica consignados en un mensaje de datos o adjuntados o lógicamente asociados al mismo tiempo que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en dicho mensaje.

En su artículo 6º dispone que cuando la Ley exija la firma de una persona ese requisito quedara 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 tan fiable como resulte apropiado a los fines para los cuales se genero o comunico ese mensaje; una firma se considera fiable si, los datos de creación de la misma en el contexto que son utilizados corresponden y están bajo control exclusivamente del firmante, por lo que es posible detectar cualquier alteración de la firma o la información, hecha después del momento de la misma.[77]

1.6.2 Comunidad Europea

La Comunidad Europea es uno de los principales impulsores de la llamada sociedad de la información, aunque tomemos en cuenta que sus propuestas no

[77] Ídem.

tienen más alcance que a los países miembros de la Unión, así que esto limita los avances a los que se ha llegado en gran parte del continente europeo.

Sobre el comercio internacional se ha emitido la Propuesta de Directiva del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, relativa a aspectos jurídicos del comercio electrónico en el mercado interior y en el área de la firma electrónica, esta tiene por objeto establecer un marco legal homogéneo que permita el desarrollo del Comercio Electrónico dentro de la Unión Europea, eliminando obstáculos legales que todavía existen en materia de prestación de servicios on-line. [78]

Según establece el artículo 1º de la presente Directiva esta tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico, además crea un marco jurídico tanto para la firma electrónica como para otros servicios de certificación.

Siguiendo con este mismo artículo la presente Directiva no regula otros aspectos relacionados con la celebración y válidez de los contratos u otras obligaciones legales cuando existen requisitos de forma establecidos en las legislaciones nacionales o comunitarias que rigen el uso de documentos.

En su artículo 2º se define entre otros conceptos a la firma electrónica como “los datos en forma electrónica ajenos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación y que debe cumplir con los siguientes requisitos”:

- “Debe estar vinculada al signatario de manera única

[78] Recordemos que los países que integran a la Unión Europea son Bélgica, Holanda, Luxemburgo, Alemania, Francia, Italia, Inglaterra, Dinamarca, Noruega, Grecia, España y Portugal.

- Permitir la identificación del signatario

- Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control.

- Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos".

También define:

- "Dispositivo de creación de firma: datos únicos como códigos o claves criptográficas privadas o un dispositivo físico de configuración única que el signatario utiliza para crear la firma digital.

- Dispositivo de verificación de firma: datos únicos, como códigos o claves criptográficas públicas o un dispositivo físico de configuración única utilizado para verificar la firma electrónica.

- Certificado reconocido de firma: certificado digital que vincula un dispositivo de verificación de firma a una persona y confirma su identidad y que cumple los requisitos establecidos en el anexo de esta Directiva".

Los efectos jurídicos de la firma electrónica en la Comunidad Europea según su artículo 5º son los siguientes:

- "Los Estados miembros procuraran 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.

b) Sea admisible como prueba en procedimientos judiciales".

Los Estados miembros velaran por que no se niegue la eficacia jurídica ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho de que esta se presente en forma electrónica no se base en un certificado reconocido o en un certificado expedido por un proveedor de servicios de certificación acreditado o que no este creada por un dispositivo seguro de creación de firma.

En cuanto a la supervisón y control el artículo 9º establece que ” la Comisión Europea estará asistida por un comité denominado “Comité de Firma Electrónica” de carácter consultivo compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión Europea”.

En relación con la protección de datos en el artículo 8º se contempla el que “los Estados miembros cuiden que los proveedores de servicios de certificación únicamente puedan recabar datos personales directamente del titular de los mismos y sólo con el alcance necesario a efectos de la expedición del certificado esos datos no podrán obtenerse o tratarse con fines distintos sin el consentimiento de su titular.

Por lo tanto es deber de los prestadores de servicios de certificación el que utilicen sistemas dignos de confianza y productos de firma electrónica que garanticen la protección contra toda alteración de los mismos que posibilite su uso con fines diferentes de aquellos para los que fueron concebidos también deberán usar productos de firma electrónica que garanticen la seguridad técnica y criptográfica de los procesos de certificación sustentadas por los productos.

Aunado a lo anterior en el artículo 6º de esta Directiva en cuanto a las responsabilidades por daños y perjuicios se establece que ” los Estados miembros

cuidaran por que el proveedor de servicios de certificación que expidan certificados reconocidos sea responsable ante cualquier persona que de buena fe confíe en el certificado a efectos de la veracidad de toda la información contenida en el certificado reconocido a partir de la fecha de su expedición; asimismo la conformidad con todos los requisitos en la expedición del certificado reconocido; igualmente la garantía de que en el momento de la expedición del certificado reconocido que obra en poder de la persona identificada en el mismo dispositivo de creación de firma correspondiente al dispositivo de verificación dado o identificado en el certificado en caso de que el proveedor de servicios de certificación genere los dispositivos de creación y de verificación de firma la garantía de que ambos funcionen conjunta y complementariamente".

El proveedor de servicios de certificación no será responsable de eventuales inexactitudes en el certificado reconocido que resulten de la información que le fue facilitada por la persona a quien se le expidió, a condición de que el proveedor demuestre haber actuado con la mayor diligencia; tampoco es responsable de daños o perjuicios causados por el uso indebido de un certificado.

Por último el reconocimiento de certificados extranjeros consiste en que los Estados miembros vigilaran por que los certificados expedidos por un proveedor de servicios de certificación establecido en un tercer país gocen de equivalencia legal con los expedidos por un proveedor de servicios de certificación establecido en la Comunidad si se cumple que:

- "El proveedor de servicios de certificación cumple los requisitos establecidos en la presente Directiva y ha sido acreditado en el marco de un sistema voluntario de acreditación establecido por un estado miembro.

- Un proveedor de servicios de certificación establecido en la Comunidad que cumpla las prescripciones del Anexo II avala el certificado en la misma medida que los suyos propios.

- El certificado o el proveedor de servicios de certificación están reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

- La Comisión podrá tomar medidas a fin de facilitar tanto la prestación de servicios de certificación transfronterizos con terceros países como el reconocimiento legal de las firmas electrónicas originarias de estos últimos, la Comisión presentara en su caso propuestas para la aplicación de normas y acuerdos internacionales relacionados con los servicios de certificación. Llegado el caso, presentara propuestas al Consejo en solicitud de mandatos de negociación de acuerdos bilaterales y multilaterales con terceros países y organizaciones internacionales". [79]

[79] FERNÁNDEZ DELPECH, Horacio, op cit.

CAPITULO II

MARCO LEGAL

2.1 Constitución Política de los Estados Unidos Mexicanos

2.2 Reformas del año 2000-2004
- 2.2.1 Código Civil Federal
- 2.2.2 Código Federal de Procedimientos Civiles
- 2.2.3 Código Civil para el Distrito Federal
- 2.2.4 Código de Procedimientos Civiles para el Distrito Federal
- 2.2.5 Código de Comercio
- 2.2.6 Código Fiscal de la Federación
- 2.2.7 Ley Federal de Protección al Consumidor
- 2.2.8 Reglas para el Registro Público De Comercio

CAPÍTULO II. MARCO LEGAL

2.1 Constitución Política de los Estados Unidos Mexicanos

Sabemos que las disposiciones contenidas en la Constitución Política de los Estados Unidos Mexicanos son las normas supremas que regulan la vida jurídica de nuestro país, y con relación al tema que nos ocupa podemos decir que la Constitución establece garantías de seguridad jurídica, en el artículo 16 donde consagra las garantías individuales que brindan a los gobernados la certeza jurídica, siendo entonces una extensión del principio de legalidad por que complementa a las garantías individuales en ese sentido; es el artículo 14 el que contiene ésta prerrogativa de los gobernados; y los efectos jurídicos de las normas que se van a examinar en sus términos, en este dispositivo el constituyente estableció los requisitos que deben de satisfacer los actos de autoridad para que sean válidos y por lo tanto produzcan efectos jurídicos lícitos.

Entonces el artículo 16 Constitucional tiene como fin el señalar los elementos de validez de los actos de autoridad, con independencia de que se afecte o no la esfera jurídica de los gobernados, tales formalidades son:

a) Que se exprese por escrito
b) Que sea dictado por autoridad competente
c) Que se funde y motive.[80]

---

[80] RABASA O. Emilio y CABALLERO Gloria, *Mexicano esta es tu Constitución*, undécima edición LVI Legislatura, Cámara de Diputados del H Congreso de la Unión, Grupo Editorial Porrua, México 1997 págs. 66-74.

El mandamiento debe ser escrito según el inciso a) por que en términos constitucionales la voluntad del Estado adquiere la calidad de acto de autoridad siempre y cuando sea manifestado por escrito, además de contener la firma autógrafa de quien representa legalmente a la autoridad.

En relación con el inciso b) este debe ser emitido por una autoridad competente, entendiendo esta competencia como la facultad que la ley brinda al poder público para satisfacer las necesidades sociales para las que fue creada, es decir con fundamento en la legitimidad del nombramiento del servidor público que representa al órgano del Estado.

Por último debe estar debidamente fundado y motivado entendiendo por la primera la exigencia constitucional que obliga al titular del órgano del estado a señalar en su mandamiento el artículo de la legislación que establece su esfera de competencia y que se considera aplicable al caso expresando los motivos que prescindan su emisión y entendiendo por motivación que los motivos indicados sean reales, ciertos y bastantes para provocar el acto de autoridad.

Una vez establecido lo anterior podemos considerar agregar al texto de la Constitución en relación con el uso de los medios electrónicos lo siguientes:

- **Artículo 8.-** En materia de derecho petición: “Los funcionarios y empleados públicos respetaran el ejercicio del derecho de petición, siempre que este se formule por escrito o a través de medios electrónicos. . . A toda petición deberá recaer un acuerdo escrito o por medios electrónicos de la autoridad.. . . “
- **Artículo 16.-** en materia de garantía de legalidad: “Nadie puede ser molestado en su persona, familia, domicilio, papeles, archivos

> electrónicos o posesiones. . . “ en toda orden de cateo, que solo la autoridad judicial podrá expedir, y que será escrita, se expresara el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetivos que se buscan, inclusive cuando se encuentren en medios electrónicos, a los que únicamente debe limitarse la diligencia. . . Las comunicaciones privadas, incluyendo las que se realicen a través de medios electrónicos, son inviolables. . . La autoridad administrativa podrá practicar visitas domiciliarias, únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policía; y exigir la exhibición de los libros y papeles y demás archivos o registros electrónicos, para comprobar que se han acatado las disposiciones fiscales. . . “

Podemos señalar que en la mayoría de los cuerpos normativos vigentes prácticamente no hay uno solo que no mencione la firma autógrafa o simplemente a la firma en general, por lo tanto haré un análisis del marco legal que trata de regular a la firma en diversos ámbitos que contemplen nuestros ordenamientos, desde las importantes reformas de mayo de 2000 hasta otras que han surgido en diferentes materias.

2.2 Reformas del año 2000 - 2004

Es muy cierto que en nuestro país se maneja desde hace algunos años, el uso de la informática para algunas transacciones principalmente en materia mercantil, pues desde al Código de Comercio de 1884 ya existían disposiciones

relativas al telégrafo como medios de comunicación; el Código Civil de 1928 ya se refería al teléfono; en algunas leyes Bancarias de 1990 incorporaron los medios telemáticos; la Ley de Protección al Consumidor de 1992 protege a los consumidores en las ventas hechas a distancia o telemarketing.

La legislación que existía hasta 1999 requería para la validez del acto o contrato del soporte en forma escrita y la forma autógrafa para vincular a las partes en forma obligatoria; así que la necesidad de modernizar la legislación mexicana para el reconocimiento jurídico de las transacciones hechas a través de Internet derivo que después de varias iniciativas y proyectos previos al Decreto que analizaremos más adelante.[81]

Así que ante la consideración generalizada sobre la conveniencia de adecuar a la legislación mexicana para dar seguridad jurídica en el uso de medios electrónicos y con base en las iniciativas de reformas y adiciones que hemos referido, tomando en cuenta los principios contenidos en los mismos, las Comisiones Unidas de Justicia y Comercio de la Cámara de Diputados presentaron para su discusión y en su caso aprobación el Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito

[81] Antecedentes: **a)** Iniciativa de reforma y adiciones a diversas disposiciones del Código de Comercio, presentado por el diputado Humberto Treviño Landois del PAN; **b)** Iniciativa que reforma y adiciona diversas disposiciones del Código de Comercio para el Distrito Federal en materia común y para toda la República en materia federal presentada por el mismo diputado que la anterior de abril de 1999 y; **c)** Iniciativa de Decreto que reforma y adiciona a diversas disposiciones del Código Civil para el Distrito Federal en materia común y para toda la República Mexicana en materia federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor, presentada por el diputado Rafael Oceguera Ramos del PRI en marzo de 2000. Cabe mencionar que estas 2 Iniciativas de reforma y la Iniciativa de Decreto que reforma, toman como base al la Ley Modelo de la UNCITRAL, de la que se hizo un estudio detallado adecuando algunas de sus disposiciones a la legislación y práctica comercial mexicana AMECE, A.C Iniciativas presentadas previas al Decreto de Reforma de 2000 [En línea]. Disponible: http://www.amece.com.mx, 14 abril de 2006.

Federal en materia común y para toda la República en materia federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor.[82]

Esta reforma en su exposición de motivos se destaca que el rápido desarrollo de los sistemas informáticos y de comunicación han llevado a buscar maneras más rápidas para llevar acabo la actividad comercial. Para poder realizar las transacciones en necesario que se contemplen como medios jurídicamente validos los documentos enviados vía electrónica. Se tomo como base jurídica la ley Modelo en materia de Comercio Electrónico de la Comisión de las Naciones Unidas. Esta ley es una serie de normas jurídicas de carácter internacional. En el marco de esta modernización a las leyes comerciales buscando por la presente:

- Eliminar los obstáculos existentes parta el comercio electrónico, ajustando la practica comercial con la Ley en dicha materia, e

- Incluir los avances y a características especificas relacionadas con el comercio electrónico, como lo es la posibilidad de acceder a los productos en fotos vía Internet sin necesidad de tener el producto físicamente presente para evaluarlo.

Dicha actualización legislativa se da en esta iniciativa bajo un marco de "neutralidad del medio", es decir, eliminando las barreras al comercio electrónico, sin modificar los requisitos en cuanto a los documentos en papel.

---

[82] DIARIO OFICIAL DE LA FEDERACIÓN, *Reformas y adiciones diversas disposiciones del Código Civil para el Distrito Federal en materia común y para toda la República en materia federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor,* Publicado el día 29 mayo de 2000.

La iniciativa logra lo anterior mediante la utilización del concepto del "equivalente funcional" entre los documentos consignados en papel y aquellos consignados por vía electrónica. Este concepto hace posible establecer una serie de características que dan a la documentación, vías medios electrónicos, un grado de seguridad similar a de la documentación en papel. La presente iniciativa busca permitir o facilitar el comercio electrónico dando igualdad de trato a los contratos que tengan soporte informático con relación a aquellos que lo basen en documentación consignada en papel.

La firma electrónica es aquella que representa el consentimiento de una de las partes para la realización de una cierta acción. Sin un régimen de firmas electrónicas y métodos confiables para la autenticación de las mismas se hace más difícil la actividad del comercio electrónico. Es por ellos que, a manera de complemento, se introduce el Titulo Segundo dentro de esta iniciativa, en el cual se presentan los lineamientos generales para la utilización y verificación de las firmas electrónicas. Este régimen de firmas electrónicas presenta la figura de las entidades certificadoras, que tienen la función de dar seguridad al régimen de corroborar la autenticidad de una firma electrónica en caso de que alguna de las partes no confíe en la originalidad de la misma.[83]

El objetivo de dichas reformas es el regular la oferta por medios electrónicos y ópticos previniendo la utilización de cualquier tecnología; dichas reformas son muy genéricas ya que mencionan medios electrónicos, ópticos y cualquier otra tecnología quedando abierta la posibilidad de regular con las

[83] Ídem.

mismas leyes desde una operación mercantil vía telefónica, compra por televisión, incluso el telefax y hasta las operaciones vía Internet.

Tomando como base el **"DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CÓDIGO CIVIL PARA EL DISTRITO FEDERAL EN MATERIA COMÚN Y PARA TODA LA REPÚBLICA EN MATERIA FEDERAL, DEL CÓDIGO DE PROCEDIMIENTOS CIVILES, DEL CÓDIGO DE COMERCIO Y DE LA LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR",** de mayo de 2000, examinaremos cada una de las disposiciones de las que habla tal Decreto respetando su texto original y analizando cada una de las reformas.

2.2.1 Código Civil Federal

Este Decreto comienza estableciendo en su **". . . ARTÍCULO PRIMERO.-** Se modifica la denominación del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal y con ello se reforman sus artículos 1º, 1803, 1805, y 1811, y se le adiciona él artículo 1834 bis para quedar como sigue":

"CÓDIGO CIVIL FEDERAL

Artículo 1º.- Las disposiciones de este Código regirán en toda la República en asuntos del orden federal.

Artículo 1803.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:

I.- Será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y

II.- El tácito resultara de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o convenio la voluntad deba manifestarse expresamente

Artículo 1805.- Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicara a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de esta en forma inmediata.

Artículo 1811.- . . . Tratándose de la propuesta y aceptación hechas a través de medios electrónicos ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos.

Artículo 1834 bis.- Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología siempre que la información generada o comunicada en forma integra a través de dichos medios sea atribuible a personas obligadas y accesible pata su ulterior consulta. En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, este y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la

información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o cualquier otra tecnología, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión integra de la misma para su ulterior consulta, otorgando a dicho instrumento de conformidad con la legislación aplicable que lo rige"[84]

En esta reforma es de destacarse:

- La importancia de esta, en donde se contemplan a los medios electrónicos, enmarcados en el concepto jurídico de mensajes de datos, para exteriorizar un consentimiento (al que también refiere como expreso y tácito), el que implica manifestación de la voluntad para someterse a una obligación;

- Se deja la puerta abierta para incorporar a la firma electrónica a nuestro sistema jurídico no solo en actividades comerciales sino para todo tipo de contrataciones;

- El mensaje de datos tiene la misma validez y cumple el requisito de la forma escrita que se exige para la formación de contratos y demás documentos legales que deben ser firmados por las partes;

- Importante reconocer la validez de la oferta y aceptación o rechazo de esta a través de mensajes de datos; lo anterior se cumple cuando la oferta se haga a una persona presente sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente, la misma regla se

[84] Ídem

aplica a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología, que permita la expresión de la oferta y la aceptación de esta en forma inmediata, no necesitando estipulación previa entre los contratantes para que estos produzcan efectos;

- Los supuestos previstos en la reforma se tendrán por cumplidos mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma integra a través de dichos medios sea atribuible a las personas que se obligaron y accesible par su ulterior consulta;

- En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante un Fedatario Público, este y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes decidieron obligarse mediante la utilización de medios electrónicos ópticos o de cualquier otra tecnología, en cuyo caso el Fedatario deberá hacer constar en el propio instrumento los elementos a través de los que se atribuye dicha información a las partes, es decir debe asentar la forma en que los datos le fueron presentados, y conservar bajo su resguardo una versión integra de la misma para su ulterior consulta, otorgando de acuerdo con la legislación aplicable que lo rige; considerando entonces una reforma a la Ley del Notariado para regular esa obligación de los notarios por tratarse de un detalle de carácter técnico.

- En particular en él artículo 1811 es acertado al establecer que no se requiere estipulación previa para que surtan sus efectos la propuesta y aceptación hecha a través de medios electrónicos por que elimina la necesidad de celebrar

cualquier tipo de contrato por escrito en este tipo de contrataciones lo que ahorra tiempo y dinero para las partes.

Además de los avances también veamos las omisiones de este ordenamiento:

- En él artículo 1834 es necesario precisar términos como la de las atribuciones de los mensajes de datos, ya que menciona a la forma escrita como una forma del consentimiento sin embargo no menciona el concepto de firma electrónica y en su lugar menciona a la forma escrita por medios electrónicos, dejando por otra parte al arbitrio de las partes el determinar y probar que el mensaje de datos fue generado, enviado, archivado, recibido o comunicado, situación que podría generar controversias y vacíos jurídicos.

- Tampoco podría aplicar él capítulo de contratos en particular por que el acto jurídico ante el que nos encontramos tiene características especiales, además de que no toda la información que se intercambia vía electrónica lleva intrínseca un acto de comercio, existen igual mensajes de datos de carácter informativo que pueden generar derechos y obligaciones.

2.2.2 Código Federal de Procedimientos Civiles

A este Código se le reformo solo un artículo contenido en el Artículo Segundo de esta reforma para quedar como sigue:

“. . . ARTÍCULO SEGUNDO.- Se adiciona él artículo 210-A al Código Federal de Procedimientos Civiles en los términos siguientes”:

"Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimara primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada, y en su caso, si es posible atribuir a las personas obligada el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquiera otra tecnología, se ha mantenido integra e inalterada a partir del momento en que se genero por primera vez en su forma definitiva y esta pueda ser accesible par su ulterior consulta." [85]

De esta reforma se destaca:

- Que se reconoce como prueba la información generada por medios electrónicos;

- Se reconocen los defectos jurídicos, validez y fuerza probatoria de los mensajes de datos, aunado a esto reconoce los requisitos de autenticidad, integridad y confiabilidad de la información generada a través de mensajes de datos;

[85] Ídem

- Por lo anterior trata de otorgar a las partes seguridad y protección jurídica para que sus conflictos puedan ser dirimidos ante un juez que usara esa información cara conformar su criterio jurídico y así en consecuencia pueda emitir una sentencia;

- La información deberá ser valorada para comprobar la fiabilidad de los métodos en que esta haya sido generada, comunicada, recibida o archivada, además si esta es posible atribuirla a las personas que se obligaron y si es accesible para su ulterior consulta;

- De lo anterior se debería proponer la implementación de autoridades de certificación para satisfacer algunos requisitos antes mencionados;

Sin embargo omite:

- Establecer mecanismos y parámetros a que se sujetaran las partes, y al no cumplir lo anterior se sujetan al arbitrio del juzgador, lo que no siempre es lo mejor;

- Menciona él termino información, pero no se refiere a la forma en que la firma digital será admitida como medio de prueba;

- Al mencionar que cuando la ley requiera que un documento sea conservado y presentado en su forma original, no establece en forma directa la obligación explicita para conservar mensajes de datos;

- Debería precisar los métodos de generación, comunicación, recepción y archivo de información.

2.2.3 Código Civil para el Distrito Federal

En la reforma hecha en mayo de 2000, se modifican artículos tanto del Código Civil Federal como del Código Civil para el Distrito Federal, es decir se hicieron las mismas reformas en ambos Códigos a los artículos 1803, 1805, tratados en el punto 2.2.1 de esta tesis, en este último ordenamiento existen otros artículos que hacen referencia también a la firma y que son los siguientes:

"TITULO CUARTO

DEL REGISTRO CIVIL

CAPÍTULO I. DISPOSICIONES GENERALES

Artículo 44.- Cuando los interesados no pudieren concurrir personalmente, podrán hacerse representar por un mandatario especial para el acto, cuyo nombramiento conste por lo menos en instrumento privado otorgado ante dos testigos. En los casos de matrimonio o de reconocimiento de hijos, se necesita poder otorgado en escritura pública o mandato extendido en escrito firmado por el otorgante y dos testigos y ratificadas las firmas ante Notario Público, Juez de lo familiar o de Paz.

LIBRO TERCERO

DE LAS SUCESIONES

TITULO SEGUNDO

DE LA SUCESIÓN POR TESTAMENTO

CAPÍTULO II. DE LA CAPACIDAD PARA TESTAR

Artículo 1311.- Firmaran el acta, además del notario y de los testigos, el juez y los médicos que intervinieron para el reconocimiento, poniéndose

al pie del testamento, razón expresa de que durante todo el acto conservo el paciente perfecta lucidez de juicio y sin este requisito y su constancia será nulo el testamento.

TITULO TERCERO

DE LA FORMA DE LOS TESTAMENTOS

CAPÍTULO II. DEL TESTAMENTO PUBLICO ABIERTO

Artículo 1512.- El testador expresara de modo claro y terminante su voluntad al notario. El notario redactara por escrito las cláusulas del testamento, sujetándose estrictamente a la voluntad del testador las leerá en voz alta para que este manifieste sí esta conforme. Si lo estuviere, firmaran la escritura el testador, el notario y en su caso los testigos y él interprete, sentándose el lugar, año, mes, día y hora en que hubiere sido otorgado.

Artículo 1514.- Cuando el Testador declare que no sabe o no puede firmar el testamento, uno de los testigos firmara a su ruego del testador y este imprimirá su huella digital.

CAPÍTULO III. TESTAMENTO PÚBLICO CERRADO

Artículo 1522.- El testador debe rubricar todas las hojas y firmar al calce del testamento; pero si no supiere o no pudiere hacerlo, podrá rubricar y firmar otra persona a su ruego.

LIBRO CUARTO

DE LAS OBLIGACIONES

PRIMERA PARTE

DE LAS OBLIGACIONES EN GENERAL

TITULO PRIMERO

FUENTES DE LAS OBLIGACIONES

CAPÍTULO I. DEL CONSENTIMIENTO

Artículo 1811.- La propuesta y aceptación hechas por telégrafo producen efectos si los contratantes con anterioridad habían estipulado por escrito esta manera de contratar, y si los originales de los respectivos telegramas contienen las firmas de los contratantes y los signos convencionales establecidos entre ellos.

FORMA

Artículo 1834.- Cuando se exija la forma escrita para el contrato, los documentos relativos deben ser firmados por todas las personas a las cuales se imponga esa obligación.

Si alguna de ellas no puede o no sabe firmar, lo hará otra a su ruego y en el documento se imprimirá la huella digital del interesado que no firmo.

TITULO SEGUNDO

DE LA COMPRAVENTA

CAPÍTULO VIII. DE LA FORMA DEL CONTRATO DE COMPRAVENTA

Artículo 2318.- Si alguno de los contratantes no supiere escribir, firmara a su nombre y a su ruego otra persona con capacidad legal, no pudiendo firmar con ese carácter ninguno de los testigos, observándose lo dispuesto en el párrafo segundo del artículo 1834.

TITULO NOVENO

DEL MANDATO

CAPÍTULO I. DISPOSICIONES GENERALES

Artículo 2551.- El mandato escrito puede otorgarse:

I. En escritura pública

II. En escrito privado, firmado por el otorgante y dos testigos y ratificadas las firmas ante notario público, Juez de Primera Instancia, Juez de Paz, o ante el correspondiente funcionario o empleado administrativo, cuando el mandato se otorgue para asuntos administrativos; y

III.- En carta poder sin ratificación de firmas.

Artículo 2555.- El mandato debe otorgarse en escritura pública o en carta poder firmada ante dos testigos y ratificadas las firmas del otorgante y testigos ante notario, ante los jueces o autoridades administrativas correspondientes:

. . . **III.** Cuando en virtud de él se haya de ejecutar el mandatario a nombre del mandante, algún acto que conforme a la ley debe constar en instrumento público".[86]

Como podemos ver fuera de las reformas de mayo de 2000 algunos otros artículos del Código Civil del Distrito Federal también hacen mención de la firma como en el Registro Civil que refiere que cuando los interesados no pudieran concurrir personalmente puede hacerlo alguien más en su nombre, dejando abierta la posibilidad de que ante cualquier comparecencia de cualquier tipo, pero

[86] CÓDIGO CIVIL PARA EL DISTRITO FEDERAL, Agenda Civil del Distrito Federal, Ediciones Fiscales ISEF, cuarta edición, México 2003, págs 6, 144, 163, 164, 192, 194, 241 y 272.

cuando se trate de matrimonio y reconocimiento de hijos el representante debe tener un mandato especial, ratificado ante Notario.

En materia de sucesiones, en la capacidad de testar el Notario y dos testigos harán constar que el testador se encontraba en pleno juicio de lo que el Notario asienta una razón ya que sin esta el testamento seria nulo, en cuanto a los tipos de testamentos existentes en el Código Civil menciona por un lado que el testamento público abierto contiene la voluntad del testador y el Notario es el encargado de redactar tal voluntad del interesado, en este caso si este último esta de acuerdo firma el testamento, debiéndose asentar además la hora, día y lugar donde se acento.

Siguiendo con los testamentos y algunos otros actos, se dispone que si alguno de los testigos no supiera escribir, firmara otro de ellos por él, pero creo que cuando menos aunque no se menciona explícitamente deberá constar la firma entera de dos testigos.

Por último en materia de contratos disponen que cuando entre los contratantes acuerden comunicarse usando alguna vía tecnológica, su consentimiento producirá efectos entre ellos, ya que una vez firmado un contrato entre ambos quedan obligados, en la compraventa en caso de que alguna parte no sepa o no puede firmar el contrato lo puede firmar otro en su representación, para lo cual o puede firmar a su ruego o mediante un mandato el que solo es valido si consta en escritura pública y esta se encuentra firmada y ratificada.

2.2.4 Código de Procedimientos Civiles para el Distrito Federal

En legislación procesal civil en México, la firma es un requisito de formalidad tanto en las peticiones de los gobernados como en las resoluciones de autoridades de primera y segunda instancia las que deberán asentar su firma autógrafa entera en cada una de sus resoluciones, tomando en cuenta que en criterio de la Suprema Corte de Justicia de la Nación la falta de este formalismo trae aparejada la nulidad de las actuaciones, así que notando lo anterior en algunos artículos del Código Civil de Procedimientos pero para el Distrito Federal se menciona esa formalidad en la siguiente forma:

"TITULO SEGUNDO

REGLAS GENERALES

CAPÍTULO II. DE LA CAPACIDAD Y PERSONALIDAD

Artículo 56.- Todos los expedientes se formaran por el tribunal con la colaboración de las partes, terceros y demás interesados y auxiliares que tengan que intervenir él los procedimientos, observando forzosamente las siguientes reglas:

I. Todos los ocursos de las partes y actuaciones judiciales deberán escribirse en español y estar firmados por quienes intervengan en ellos. Cuando alguna de las partes no supiere o no pudiere firmar impondrá su huella digital, firmando otra persona en su nombre y a su ruego, indicando estas circunstancias. La falta de cumplimiento a los requisitos señalados, dará lugar a que no se obsequie la petición que se convenga en el escrito respectivo.

CAPÍTULO V. DE LAS NOTIFICACIONES

Artículo 124.- Debe firmar las notificaciones la persona que las hace y aquélla a quien se hacen. Si esta no supiere o no quisiere firmar, lo hará constar el secretario o notificador. A toda persona se le dará de inmediato copia simple de la resolución que se le notifique o de la promoción o diligencia a la que le hubiere recaído, bastando la petición verbal de su entrega....."

TITULO QUINTO

ACTOS PREJUDICIALES

CAPÍTULO II. MEDIOS PREPARATORIOS DEL JUICIO EJECUTIVO

Artículo 202.- Se tendrá por reconocido el documento privado que contenga deuda liquida y sea de plazo cumplido, cuando el deudor reconozca su firma ante la presencia judicial o cuando requerido para ello rehusé contestar si es o no suya la firma y cuando deje de asistir a la audiencia de reconocimiento sin causa justa.

Artículo 203.- Puede hacerse el reconocimiento de documentos firmados ante notario, ya en el momento del otorgamiento con posterioridad, siempre que lo haga la persona directamente obligada, su representante legitimo o su mandatario con poder bastante.

El notario hará constar el reconocimiento al pie del documento mismo asentando si la persona que reconoce es apoderado del deudor y la cláusula relativa.

TITULO SEXTO

DEL JUICIO ORDINARIO

CAPÍTULO I. DE LA DEMANDA, CONTESTACIÓN Y FIJACIÓN DE LA CUESTIÓN

Artículo 255.- Toda contienda judicial principiara por demanda, en cual se expresaran: . . . I a VII

. . . **VIII.** La firma del actor, o de su representante legitimo. Si estos no supieren o no pudieren firmar pondrán su huella digital firmando otra persona en su nombre y a su ruego, indicando estas circunstancias.

Artículo 260.- El demandado formulará la contestación a la demanda en los siguientes términos: . . . I a III

IV. Se asentara la firma del puño y letra del demandado o de su representante legitimo. Si estos no supieren o no pudieren firmar, lo hará un tercero en su nombre y a su ruego, indicando estas circunstancias, poniendo los primeros su huella digital.. . . V a VII.

CAPÍTULO IV

SECCIÓN III

DE LA PRUEBA INSTRUMENTAL

Artículo 339.- Solo pueden reconocer un documento privado el que lo firma, el que lo manda extender o él legitimo representante de ellos con poder o cláusula especial.....

Artículo 341.- Podrá pedirse el cotejo de firmas y letras, siempre que se niegue o que se ponga en duda la autenticidad de un documento privado o de un documento público que carezca de matriz.....

Artículo 343.- Se consideraran indubitables para el cotejo:

I. . . . **II.** Los documentos privados cuya letra o firma haya sido reconocida en juicio por aquel a quien se atribuya la dudosa;

III. Los documentos cuya letra o firma ha sido judicialmente declarada propia de aquél a quien se atribuye la dudosa;. . IV. . . .

V. Las firmas puestas en actuaciones judiciales, en presencia del secretario del tribunal, por la parte cuya firma o letra se trata de comprobar.

TITULO SÉPTIMO

DE LOS JUICIOS ESPECIALES Y DE LA VÍA DE APREMIO

CAPÍTULO II. DEL JUICIO EJECUTIVO

SECCIÓN I

REGLAS GENERALES

Artículo 443.- Para que el juicio ejecutivo tenga lugar se necesita un título que lleve aparejada ejecución. Traen aparejada ejecución: I a III....

IV. Cualquier documento privado después de reconocido por quien lo hizo o lo mando extender; basta con que se reconozca la firma aún cuando se niegue la deuda.. . . V a VIII

TITULO DECIMOCUARTO

JUICIOS SUCESORIOS

CAPÍTULO IX. DEL TESTAMENTO PÚBLICO CERRADO

Artículo 877.- Para la apertura del testamento cerrado, los testigos reconocerán separadamente sus firmas y el pliego que las contenga. El representante del Ministerio Público asistirá a la diligencia.

Artículo 878.- Cumplido lo prescrito en sus respectivos casos en los artículos del código civil números 1542 a 1547, el Juez, en presencia del notario, testigos, representante del ministerio Público y secretario, abrirá el testamento, lo leerá en voz alta, omitiendo lo que debe permanecer en secreto.

Enseguida firmaran al margen del testamento las personas que hayan intervenido en la diligencia, con el juez y el secretario, y se le pondrá el sello del juzgado, asentándose acta de todo ello".[87]

Sabemos que la capacidad es uno de los requisitos para contratar y obligarse así que los que intervengan en cualquier actuación judicial deben expresarse en idioma español y firmando sus actuaciones, si alguna de las partes no sabe firmar ese requisito se subsana mediante la huella digital, la falta de este requisito podrá hacer que no se cumpla alguna petición hecha a la autoridad.

En cuanto a las notificaciones estas deben ir firmadas tanto por la persona que las hace como de quien recibe esa notificación.

En el aspecto contencioso, se tiene por reconocido el documento privado que contenga deuda, cuando el deudor reconozca su firma ante la presencia judicial o cuando requerido para ello rehusé contestar si es o no suya la firma.

En materia procesal la contienda inicia con la demanda, la que entre otros requisitos que señala él artículo 255 de este Código, requiere que contenga la firma del actor o de su representante, si hubiera el caso de no saber firmar, podrán poner su huella digital o firmar otra persona en su representación; por su parte el

[87] CÓDIGO De PROCEDIMIENTOS CIVILES PARA EL DISTRITO FEDERAL, Agenda Civil del Distrito Federal, Ediciones Fiscales ISEF, cuarta edición, México 2003, págs 11, 31, 49, 55, 56, 69, 84 Y 154.

demandado contestara la demanda el que también debe firmarla de puño y letra o su representante.

Procesalmente solo pueden reconocer un documento privado el que lo firma, el que lo manda extender o él legitimo representante de ellos.

En caso de impugnación quien pida el cotejo debe señalar el documento indubitable, o pedirá al tribunal que cite al interesado para que en su presencia ponga la firma o letras que servirán para el cotejo.

Es requisito que los documentos en que se base de la acción como aquellos que traen aparejada ejecución contengan la firma autógrafa, la escritura de petición y contratos de cualquier tipo deben tener la firma de todos los interesados.

En materia de juicios sucesorios también contempla para el caso de testamentos cerrados, que se necesitara que los testigos reconozcan sus firmas por separado para proceder a conocer el contenido de ese testamento.

2.2.5 Código de Comercio

En este Código sufrió importantes reformas en los años de 2000 y 2003, en materia de Comercio Electrónico y en materia de Firma Electrónica respectivamente; examinaremos primero la reforma de mayo de 2000 en la que se contienen importantes innovaciones que no solo tienen que ver con la materia mercantil, sino también se incluyen novedades sobre el Registro Público de

Comercio[88], pero nos avocaremos primero las reformas hechas al Libro Segundo del Código de Comercio en materia de Comercio Electrónico, y que precisamente resultaron de la siguiente manera:

". . . ARTÍCULO TERCERO.- Se reforman los artículos 18, 20, 21 párrafo primero, 22, 23, 24, 25, 26, 27, 30, 31, 32, 49, 80 y 1205, y se adicionan los artículos 20 bis, 21 bis, 21 bis 1, 30 bis, 30 bis 1 y 32, 1298-A; el Titulo II que se denominará "Del Comercio Electrónico" que comprenderá los artículos 89 a 94, y se modifica la denominación del Libro Segundo del Código de Comercio, disposiciones todas del referido Código de comercio para quedar como sigue:

"LIBRO SEGUNDO

DEL COMERCIO EN GENERAL

Artículo 80.- Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedaran perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que esta fuere modificada.

TITULO II

DEL COMERCIO ELECTRÓNICO

Artículo 89.- En los actos de comercio podrán emplearse los medios electrónicos ópticos o cualquier otra tecnología. Par efecto del presente Código a la información generada, enviada, recibida, archivada o

[88] Vid. Las reformas hechas al Código de Comercio que se refieren al Registro Público de Comercio en el Capítulo V punto 5.6.2, mas adelante

comunicada a través de dichos medios se le denominara mensaje de datos.

Artículo 90.- Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor si ha sido enviado:

I.- Usando medios de identificación, tales como claves o contraseñas y;

II.- Por un sistema de información programado por el emisor o en u nombre para que opere automáticamente;

Artículo 91.- El momento de recepción de la información a que se refiere él artículo anterior sé determinar como sigue:

I.- Si el destinatario ha designado un sistema de información para la recepción, esta tendrá lugar en el momento en que ingrese en dicho sistema o

II.- De enviarse a un sistema del destinatario que no sea el designado o de no haber un sistema de información designado en el momento en que el destinatario obtenga dicha información.

Para efectos de este Código, se entiende por sistema de información cualquier medio tecnológico utilizado para operar mensajes de datos.

Artículo 92.- Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos, bien sea por disposición legal o por así requerirlo el emisor, se considerara que el mensaje de datos ha sido enviado, cuando se haya recibido el acuse respectivo.

Salvo prueba en contrario, se presumirá que se ha recibido el mensaje de datos cuando el emisor reciba el acuse correspondiente.

Artículo 93.- Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que este sea atribuible a las personas obligadas y accesible para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, este y las partes obligadas podrán a través e mensaje de datos, expresar los términos exactos en que las partes han decidido obligarse en cuyo cayo el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión integra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo 94.- Salvo pacto en contrario el mensaje de dato se tendrá por expedido en le lugar donde el emisor tendrá su domicilio y por recibido en el lugar donde el destinatario tenga el suyo.

Artículo 1205.- Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en él animo del juzgador acerca de los hechos. Controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privado, inspección judicial, fotografías, facsímiles, cintas cinematográficas de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.

Artículo 1298 - A.- Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes sé estimar primordialmente la fiabilidad de los métodos en que haya sido generada, archivada, comunicada o conservada dicha información".

En esta reforma se destaca:

- Establece la aceptación como el momento en que se perfecciona un contrato o acuerdo generado por medios electrónicos, ópticos o de cualquier otra tecnología;

- Crea un apartado para el Comercio electrónico al cual define como aquel donde convenios y contratos por medios electrónicos serán perfeccionados desde que se aceptan;

- Establece la denominación de "mensajes de datos";

- Menciona requisitos para establecer la autoría de los mensajes, y el uso de claves o contraseñas;

- Deja abierto el uso de algún sistema de información como por ejemplo la encriptación;

- Establece el momento en que un mensaje de datos se considera recibido, obligando a quien lo recibió a expedir un acuse de recibo para que pueda surtir efectos;

- Los requisitos de forma escrita de los contratos y la firma se tendrán por cumplidos tratándose de mensajes de datos siempre que sean atribuibles a las personas obligadas y accesibles para su posterior consulta;

- Autoriza a Fedatario Público a recibir de las partes por medios electrónicos los términos en que han decidido obligarse, por lo que el fedatario debe hacer

constar en el propio instrumento los elementos a través de los cuales se atribuyen los mensajes de datos a las partes;

- Admite a los mensajes de datos como pruebas siempre que se compruebe esa fuerza probatoria mediante la fiabilidad del método en que haya sido generado;

- En el artículo 93 se estipula que se pueden tener como instrumento público medios digitales avalados por un fedatario público que según entiendo en nuestra legislación puede ser tanto un notario como un corredor público, con lo cual sabemos que cuando media un fedatario se puede contar con mayor certeza jurídica;

Las omisiones contenidas en este Decreto de reforma de mayo de 2000 se subsanaron con las reformas hechas en agosto de 2003, mediante él: **DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CÓDIGO DE COMERCIO EN MATERIA DE FIRMA ELECTRÓNICA . . .**

> **"ARTÍCULO ÚNICO:** Se reforman los artículos 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113 y 114. Se adicionan los artículos 89 bis, 90 bis, 91 bis, 93 bis. Se adicionan los Capítulos Primero, Segundo, Tercero y Cuarto al Título Segundo, denominado del Comercio Electrónico, correspondiente al Libro Segundo, todos del Código de Comercio, para quedar de la siguiente manera:

TÍTULO SEGUNDO

DEL COMERCIO ELECTRÓNICO

CAPÍTULO I. DE LOS MENSAJES DE DATOS

Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.

Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del mensaje de datos en relación con la información documentada en medios no electrónicos y de la firma electrónica en relación con la firma autógrafa.

En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones:

Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.

Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.

Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.

Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en tal mensaje, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.

En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.

Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.

Secretaría: Se entenderá la Secretaría de Economía.

Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.

Titular del Certificado: Se entenderá a la persona a cuyo favor fue expedido el Certificado.

Artículo 89 bis.- No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.

Artículo 90.- Se presumirá que un Mensaje de Datos proviene del Emisor si ha sido enviado:

I. Por el propio Emisor;

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

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

Artículo 90 bis.- Se presume que un Mensaje de Datos ha sido enviado por el Emisor y, por lo tanto, el Destinatario o la Parte que Confía, en su caso, podrá actuar en consecuencia, cuando:

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

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

Lo dispuesto en el presente artículo no se aplicará:

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

II. A partir del momento en que el Destinatario o la Parte que Confía, tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el Mensaje de Datos no provenía del Emisor.

Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del Emisor, se presumirá que se

actuó con la debida diligencia si el método que usó el Destinatario o la Parte que Confía cumple con los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas.

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

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

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

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

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

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

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

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

a) Toda comunicación del Destinatario, automatizada o no, o

b) Todo acto del Destinatario, que baste para indicar al Emisor que se ha recibido el Mensaje de Datos.

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

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

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

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

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

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

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

Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes.

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

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

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

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

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

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

Artículo 94.- Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido en el lugar donde el Emisor

tenga su establecimiento y por recibido en el lugar donde el Destinatario tenga el suyo. Para los fines del presente artículo:

I. Si el Emisor o el Destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal, y

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

Artículo 95.- Conforme al artículo 90, siempre que se entienda que el Mensaje de Datos proviene del Emisor, o que el Destinatario tenga derecho a actuar con arreglo a este supuesto, dicho Destinatario tendrá derecho a considerar que el Mensaje de Datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia. El Destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error en el Mensaje de Datos recibido.

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

CAPÍTULO II. DE LAS FIRMAS

Artículo 96.- Las disposiciones del presente Código serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una Firma Electrónica.

Artículo 97.- Cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.

La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;

II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;

III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y

IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

Artículo 98.- Los Prestadores de Servicios de Certificación determinarán y harán del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 97.

La determinación que se haga, con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 99.- El Firmante deberá:

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

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

III. Cuando se emplee un Certificado en relación con una Firma Electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el Certificado, con su vigencia, o que hayan sido consignadas en el mismo, son exactas.

El Firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en el presente artículo, y

IV. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para

impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia.

CAPÍTULO III. DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 100.- Podrán ser Prestadores de Servicios de Certificación, previa acreditación ante la Secretaría:

I. Los notarios públicos y corredores públicos;

II. Las personas morales de carácter privado, y

III. Las instituciones públicas, conforme a las leyes que les son aplicables.

La facultad de expedir Certificados no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.

Artículo 101.- Los Prestadores de Servicios de Certificación a los que se refiere la fracción II del artículo anterior, contendrán en su objeto social las actividades siguientes:

I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;

II. Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante y verificar la Firma Electrónica de quien realiza la verificación;

III. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Avanzadas y emitir el Certificado, y

IV. Cualquier otra actividad no incompatible con las anteriores.

Artículo 102.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos:

I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación;

II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad;

III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros;

IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría;

VI. Establecer por escrito su conformidad para ser sujeto a Auditoria por parte de la Secretaría, y

VII. Registrar su Certificado ante la Secretaría.

B) Si la Secretaría no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 anterior, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.

Artículo 103.- Las responsabilidades de las Entidades Prestadoras de Servicios de Certificación deberán estipularse en el contrato con los firmantes.

Artículo 104.- Los Prestadores de Servicios de Certificación deben cumplir las siguientes obligaciones:

I. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suya, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante;

II. Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica;

III. 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, en su caso, de la forma en que garantiza su posible responsabilidad;

IV. Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría;

V. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación;

VI. En el caso de cesar en su actividad, los Prestadores de Servicios de Certificación deberán comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos;

VII. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;

VIII. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el Destinatario, y

IX. Proporcionar medios de acceso que permitan a la Parte que Confía en el Certificado determinar:

a) La identidad del Prestador de Servicios de Certificación;

b) Que el Firmante nombrado en el Certificado tenía bajo su control el dispositivo y los Datos de Creación de la Firma en el momento en que se expidió el Certificado;

c) Que los Datos de Creación de la Firma eran válidos en la fecha en que se expidió el Certificado;

d) El método utilizado para identificar al Firmante;

e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los Datos de Creación de la Firma o el Certificado;

f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación;

g) Si existe un medio para que el Firmante dé aviso al Prestador de Servicios de Certificación de que los Datos de Creación de la Firma han sido de alguna manera controvertidos, y

h) Si se ofrece un servicio de terminación de vigencia del Certificado.

Artículo 105.- La Secretaría coordinará y actuará como autoridad Certificadora, y registradora, respecto de los Prestadores de Servicios de Certificación, previstos en este Capítulo.

Artículo 106.- Para la prestación de servicios de certificación, las instituciones financieras y las empresas que les prestan servicios auxiliares o complementarios relacionados con transferencias de fondos o valores, se sujetarán a las leyes que las regulan, así como a las disposiciones y autorizaciones que emitan las autoridades financieras.

Artículo 107.- Serán responsabilidad del Destinatario y de la Parte que Confía, en su caso, las consecuencias jurídicas que entrañe el hecho de que no hayan tomado medidas razonables para:

I. Verificar la fiabilidad de la Firma Electrónica, o

II. Cuando la Firma Electrónica esté sustentada por un Certificado:

a) Verificar, incluso en forma inmediata, la validez, suspensión o revocación del Certificado, y

b) Tener en cuenta cualquier limitación de uso contenida en el Certificado.

Artículo 108.- Los Certificados, para ser considerados válidos, deberán contener:

I. La indicación de que se expiden como tales;

II. El código de identificación único del Certificado;

III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;

IV. Nombre del titular del Certificado;

V. Periodo de vigencia del Certificado;

VI. La fecha y hora de la emisión, suspensión, y renovación del Certificado;

VII. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y

VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.

Artículo 109.- Un Certificado dejará de surtir efectos para el futuro, en los siguientes casos:

I. Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido. Antes de que concluya el periodo de vigencia del Certificado

podrá el Firmante renovarlo ante el Prestador de Servicios de Certificación;

II. Revocación por el Prestador de Servicios de Certificación, a solicitud del Firmante, o por la persona física o moral representada por éste o por un tercero autorizado;

III. Pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado;

IV. Por haberse comprobado que al momento de su expedición, el Certificado no cumplió con los requisitos establecidos en la ley, situación que no afectará los derechos de terceros de buena fe, y

V. Resolución judicial o de autoridad competente que lo ordene.

Artículo 110.- El Prestador de Servicios de Certificación que incumpla con las obligaciones que se le imponen en el presente Capítulo, previa garantía de audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

Artículo 111.- Las sanciones que se señalan en este Capítulo se aplicarán sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan a los delitos en que, en su caso, incurran los infractores.

Artículo 112.- Las autoridades competentes harán uso de las medidas legales necesarias, incluyendo el auxilio de la fuerza pública, para lograr la ejecución de las sanciones y medidas de seguridad que procedan conforme a esta Ley. Incluso, en los procedimientos instaurados se podrá solicitar a los órganos competentes la adopción de las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte.

Artículo 113.- En el caso de que un Prestador de Servicios de Certificación sea suspendido, inhabilitado o cancelado en su ejercicio, el registro y los Certificados que haya expedido pasarán, para su administración, a otro Prestador de Servicios de Certificación, que para tal efecto señale la Secretaría mediante reglas generales.

CAPÍTULO IV. RECONOCIMIENTO DE CERTIFICADOS Y FIRMAS ELECTRÓNICAS EXTRANJEROS

Artículo 114.- Para determinar si un Certificado o una Firma Electrónica extranjeros producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos:

I. El lugar en que se haya expedido el Certificado o en que se haya creado o utilizado la Firma Electrónica, y

II. El lugar en que se encuentre el establecimiento del Prestador de Servicios de Certificación o del Firmante.

Todo Certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que un Certificado expedido en la

República Mexicana si presenta un grado de fiabilidad equivalente a los contemplados por este Título.

Toda Firma Electrónica creada o utilizada fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que una Firma Electrónica creada o utilizada en la República Mexicana si presenta un grado de fiabilidad equivalente.

A efectos de determinar si un Certificado o una Firma Electrónica presentan un grado de fiabilidad equivalente para los fines de los dos párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente.

Cuando, sin perjuicio de lo dispuesto en los párrafos anteriores, las partes acuerden entre sí la utilización de determinados tipos de Firmas Electrónicas y Certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable".[89]

A pesar que en el 2000 se realizo una importante reforma, se dejaron muchos cabos sueltos en la forma en que operarían en nuestro país las firmas electrónicas, un punto a favor de los legisladores fue él volver a reformar aquel decreto de 2000 en 2003 para que de manera más precisa se regulara a la firma electrónica así que de esta ultima reforma es de destacarse:

[89] DIARIO OFICIAL DE LA FEDERACIÓN, Servicio de Administración Tributaria. Secretaría de Economía *Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en materia de Firma Electrónica* Publicado el 29 de agosto de 2003. [En línea]. Disponible: http://www.sat.gob.mx/, 14 abril de 2006.

- Se crean capítulos sobre temas específicos, lo que no había sucedido hasta entonces en materia legislativa, se crea un capítulo para tratar los mensajes de datos, uno para las firmas, otro para los prestadores de servicios de certificación y él ultimo para los certificados y firmas electrónicas extranjeras;

- Por fin define conceptos importantes como destinatario, emisor, firma electrónica, avanzada o fiable, firmante, intermediario, mensaje de datos, parte que confía, prestado de servicios de certificación, sistemas de información y titular del certificado;

- En él capítulo I de los mensajes de datos, determina las disposiciones que regirán en materia comercial, además del momento en que se presume que un mensaje de datos fue enviado y expedido por el emisor y recibido por el destinatario;

- Da importancia a los acuerdos a que hayan llegado las partes que intervienen tanto en emisión como e recepción de los mensajes de datos;

- Especifica que elementos se deben de cumplir para que el destinatario pueda acusar de recibido la información que le fue enviada por el emisor

- No niega los efectos jurídicos a la información generada en mensaje de datos ya que como sabemos la ley exige la forma escrita y la firma para la validez de los contratos, así que los generados vía electrónica no carecen de esta formalidad;

- Da especial cuidado a que cuando por ley se requiera que la información sea presentada y conservada en su forma original esto se cumple si hay la garantía de que se ha conservado y ha permanecido inalterada;

- En el Capítulo II que atiende especialmente a las firmas, no excluye ningún método para que se pueda crear una firma electrónica, pero define exactamente los requisitos de una firma electrónica avanzada o fiable:

- Establece las obligaciones de los firmantes;

- También en él Capítulo III que esta dedicado exclusivamente a la función de los prestadores de servicios de certificación, que podrán operar siempre y cuando tengan acreditación de la Secretaria de Economía;

- En el mismo Capítulo III contempla que los notarios entre otros fedatarios o personas morales de carácter privado e instituciones públicas puedan actuar como prestadores de servicios de certificación;

- Las Instituciones Públicas tienen la obligación de verificar la identidad de los otorgantes, comprueba la integridad de los mensajes de datos además de llevar un registro;

- Especifica las responsabilidades, obligaciones de las entidades prestadoras de servicios de certificación, con vigilancia de la secretaría de economía;

- Hace que asuman su responsabilidad los usuarios de esta tecnología y de las consecuencias jurídicas que conlleva su uso;

- Por ultimo también al igual que otos países de América Latina también reconoce el valor de los cerificados expedidos en el extranjero.

Esta reforma también omite:

- Mencionar algo referente al no repudio de la información por parte del emisor del mensaje;

- No especifica por medio de que tecnología se puede verificar que un mensaje de datos ha permanecido integro, completo o inalterado;

- Menciona las obligaciones de las Instituciones Públicas en la prestación de servicios de certificación como lo son la de verificar, comprobar o llevar registros, pero solo las limita a las Instituciones públicas no incluye a los fedatarios y personas morales de carácter privado.

2.2.6 Código Fiscal de la Federación

De acuerdo a los artículos extraídos del Código Fiscal de la Federación y publicados por la Secretaria de Hacienda y Cedito Público en el Diario Oficial del 5 de enero de 2004, en el **"DECRETO POR EL QUE SE REFORMAN, ADICIONAN Y DEROGAN DIVERSAS DISPOSICIONES DEL CÓDIGO FISCAL",** se contienen numerosas reformas en cuanto a los medios electrónicos como sabemos el Código Fiscal es un ordenamiento que es un pilar de la Legislación Tributaria en nuestro país, que no había sido reformado por los Órganos Legislativos, trayendo como consecuencia, que varias de las disposiciones tuvieran que adecuarse por el nacimiento de las nuevas tecnologías tanto de México como del mundo.

Es importante hacer mención, que, dentro de los cambios más representativos, se encuentra ahora si, la regulación de los pagos por Internet, las firmas electrónicas tanto de contribuyentes como de las autoridades, notificaciones por Internet, etc., es decir, se incorpora al cuerpo normativo, las disposiciones

necesarias, para que queden bien definidas las figuras antes expuestas, y en consecuencia, se le brinde seguridad jurídica a los contribuyentes.

Algunos de los artículos más importantes contenidos en esta reforma son los contenidos en él:

"CAPÍTULO SEGUNDO

DE LOS MEDIOS ELECTRÓNICOS

Artículo 17-C. Tratándose de contribuciones administradas por organismos fiscales autónomos, las disposiciones de este Código en materia de medios electrónicos sólo serán aplicables cuando así lo establezca la ley de la materia.

Artículo 17-D. Cuando las disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos que establezcan una regla diferente.

Las autoridades fiscales, mediante reglas de carácter general, podrán autorizar el uso de otras firmas electrónicas".

Para los efectos mencionados en este articulo, se deberá contar con un certificado que confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y de los sellos digitales previstos en el artículo 29 de este Código, y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas. El Banco de México publicará en el Diario Oficial de la Federación la denominación de los

prestadores de los servicios mencionados que autorice y, en su caso, la revocación correspondiente.

En los documentos digitales, una firma electrónica avanzada amparada por un certificado vigente sustituirá a la firma autógrafa del firmante, garantizará la integridad del documento y producirá los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio.

Se entiende por documento digital todo mensaje de datos que contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología.

Los datos de creación de firmas electrónicas avanzadas podrán ser tramitados por los contribuyentes ante el Servicio de Administración Tributaria o cualquier prestador de servicios de certificación autorizado por el Banco de México.

Cuando los datos de creación de firmas electrónicas avanzadas se tramiten ante un prestador de servicios de certificación diverso al Servicio de Administración Tributaria, se requerirá que el interesado previamente comparezca personalmente ante el Servicio de Administración Tributaria para acreditar su identidad. En ningún caso los prestadores de servicios de certificación autorizados por el Banco de México podrán emitir un certificado sin que previamente cuenten con la comunicación del Servicio de Administración Tributaria de haber acreditado al interesado, de conformidad con las reglas de carácter general que al efecto expida. A su vez, el prestador de servicios deberá informar al Servicio de Administración Tributaria el código de identificación único del certificado asignado al interesado.

La comparecencia de las personas físicas a que se refiere el párrafo anterior, no podrá efectuarse mediante apoderado o representante legal. Únicamente para los efectos de tramitar la firma electrónica avanzada de las personas morales de conformidad con lo dispuesto en el artículo 19-A de este Código, se requerirá el poder previsto en dicho artículo.

La comparecencia previa a que se refiere este artículo también deberá realizarse cuando el Servicio de Administración Tributaria proporcione a los interesados los certificados, cuando actúe como prestador de servicios de certificación.

Para los efectos fiscales, los certificados tendrán una vigencia máxima de dos años, contados a partir de la fecha en que se hayan expedido. Antes de que concluya el período de vigencia de un certificado, su titular podrá solicitar uno nuevo. En el supuesto mencionado el Servicio de Administración Tributaria podrá, mediante reglas de carácter general, relevar a los titulares del certificado de la comparecencia personal ante dicho órgano para acreditar su identidad y, en el caso de las personas morales, la representación legal correspondiente, cuando los contribuyentes cumplan con los requisitos que se establezcan en las propias reglas. Si dicho órgano no emite las reglas de carácter general, se estará a lo dispuesto en los párrafos sexto y séptimo de este artículo.

Para los efectos de este Capítulo, el Servicio de Administración Tributaria aceptará los certificados de firma electrónica avanzada que emita la Secretaría de la Función Pública, de conformidad con las facultades que le confieran las leyes para los servidores públicos, así como los emitidos por los prestadores de servicios de certificación que estén autorizados para ello en los términos del

derecho federal común, siempre que en ambos casos, las personas físicas titulares de los certificados mencionados hayan cumplido con lo previsto en los párrafos sexto y séptimo de este artículo.

"Artículo 17-E. Cuando los contribuyentes remitan un documento digital a las autoridades fiscales, recibirán el acuse de recibo que contenga el sello digital".

El sello digital es el mensaje electrónico que acredita que un documento digital fue recibido por la autoridad correspondiente y estará sujeto a la misma regulación aplicable al uso de una firma electrónica avanzada. En este caso, el sello digital identificará a la dependencia que recibió el documento y se presumirá, salvo prueba en contrario, que el documento digital fue recibido en la hora y fecha que se consignen en el acuse de recibo mencionado.

El Servicio de Administración Tributaria establecerá los medios para que los contribuyentes puedan verificar la autenticidad de los acuses de recibo con sello digital.

"Artículo 17- F. El Servicio de Administración Tributaria podrá proporcionar los siguientes servicios de certificación de firmas electrónicas avanzadas:

I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;

II. Comprobar la integridad de los documentos digitales expedidos por las autoridades fiscales;

III. Llevar los registros de los elementos de identificación y de vinculación con los medios de identificación electrónicos de los

firmantes y, en su caso, de la representación legal de los firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las firmas electrónicas avanzadas y emitir el certificado;

IV. Poner a disposición de los firmantes los dispositivos de generación de los datos de creación y de verificación de firmas electrónicas avanzadas o sellos digitales.

V. Informar, antes de la emisión de un certificado a la persona que solicite sus servicios, de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso.

VI. Autorizar a las personas que cumplan con los requisitos que se establezcan en reglas de carácter general, para que proporcionen los siguientes servicios:

a) Proporcionar información sobre los certificados emitidos por el Servicio de Administración Tributaria, que permitan a terceros conocer:

1) Que el certificado fue emitido por el Servicio de Administración Tributaria.

2) Si se cuenta con un documento suscrito por el firmante nombrado en el certificado en el que se haga constar que dicho firmante tenía bajo su control el dispositivo y los datos de creación de la firma electrónica avanzada en el momento en que se expidió el certificado y que su uso queda bajo su exclusiva responsabilidad.

3) Si los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado.

4) El método utilizado para identificar al firmante.

5) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado.

6) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad del Servicio de Administración Tributaria.

7) Si se ofrece un servicio de terminación de vigencia de los certificados.

b) Proporcionar los servicios de acceso al registro de certificados. A dicho registro podrá accederse por medios electrónicos.

Las facultades mencionadas podrán ser ejercidas directamente en cualquier tiempo por el Servicio de Administración Tributaria, pudiendo hacerlo en forma separada o conjunta con las personas autorizadas en los términos de esta fracción.

Artículo 17-G. Los certificados que emita el Servicio de Administración Tributaria para ser considerados válidos deberán contener los datos siguientes:

I. La mención de que se expiden como tales. Tratándose de certificados de sellos digitales, se deberán especificar las limitantes que tengan para su uso.

II. El código de identificación único del certificado.

III. La mención de que fue emitido por el Servicio de Administración Tributaria y una dirección electrónica.

IV. Nombre del titular del certificado y su clave del registro federal de contribuyentes.

V. Período de vigencia del certificado, especificando el día de inicio de su vigencia y la fecha de su terminación.

VI. La mención de la tecnología empleada en la creación de la firma electrónica avanzada contenida en el certificado.

VII. La clave pública del titular del certificado".

Cuando se trate de certificados emitidos por prestadores de servicios de certificación autorizados por el Banco de México, que amparen datos de creación de firmas electrónicas que se utilicen para los efectos fiscales, dichos certificados deberán reunir los requisitos a que se refieren las fracciones anteriores, con excepción del señalado en la fracción III. En sustitución del requisito contenido en dicha fracción, el certificado deberá contener la identificación del prestador de servicios de certificación y su dirección electrónica, así como los requisitos que para su control establezca el Servicio de Administración Tributaria, mediante reglas de carácter general.

"Artículo 17-H. Los certificados que emita el Servicio de Administración Tributaria quedarán sin efectos cuando:

I. Lo solicite el firmante.

II. Lo ordene una resolución judicial o administrativa.

III. Fallezca la persona física titular del certificado. En este caso la revocación deberá solicitarse por un tercero legalmente autorizado, quien deberá acompañar el acta de defunción correspondiente.

IV. Se disuelvan, liquiden o extingan las sociedades, asociaciones y demás personas morales. En este caso, serán los liquidadores quienes presenten la solicitud correspondiente.

V. La sociedad escíndete o la sociedad fusionada desaparezca con motivo de la escisión o fusión, respectivamente. En el primer caso, la

cancelación la podrá solicitar cualquiera de las sociedades escindidas; en el segundo, la sociedad que subsista.

VI. Transcurra el plazo de vigencia del certificado.

VII. Se pierda o inutilice por daños, el medio electrónico en el que se contengan los certificados.

VIII. Se compruebe que al momento de su expedición, el certificado no cumplió los requisitos legales, situación que no afectará los derechos de terceros de buena fe.

IX. Cuando se ponga en riesgo la confidencialidad de los datos de creación de firma electrónica avanzada del Servicio de Administración Tributaria".

El Servicio de Administración Tributaria podrá cancelar sus propios certificados de sellos o firmas digitales, cuando se den hipótesis análogas a las previstas en las fracciones VII y IX de este artículo.

Cuando el Servicio de Administración Tributaria revoque un certificado expedido por él, se anotará en el mismo la fecha y hora de su revocación.

Para los terceros de buena fe, la revocación de un certificado que emita el Servicio de Administración Tributaria, surtirá efectos a partir de la fecha y hora que se dé a conocer la revocación en la página electrónica respectiva del citado órgano.

"**Artículo 17-I.** La integridad y autoría de un documento digital con firma electrónica avanzada o sello digital será verificable mediante el método de remisión al documento original con la clave pública del autor.

Artículo 17-J. El titular de un certificado emitido por el Servicio de Administración Tributaria, tendrá las siguientes obligaciones:

I. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los datos de creación de la firma.

II. Cuando se emplee el certificado en relación con una firma electrónica avanzada, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el certificado, con su vigencia, o que hayan sido consignados en el mismo, son exactas.

III. Solicitar la revocación del certificado ante cualquier circunstancia que pueda poner en riesgo la privacidad de sus datos de creación de firma.

El titular del certificado será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente con las obligaciones previstas en el presente artículo". [90]

Es de destacarse en esta reforma que:

- Sé precisa que en contribuciones administradas por otros organismos, el IMSS e INFONAVIT, no les es aplicable el esquema de pagos electrónicos a menos que exista disposición expresa de la Ley.

- Se trata de facilitar el cumplimiento de las disposiciones fiscales, con el uso de medios electrónicos, lo que ahorrará tiempo y recursos en beneficio de los contribuyentes obligando a estos que cuando presenten documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor.

---

[90] CÓDIGO FISCAL DE LA FEDERACIÓN Instituto de Investigaciones Jurídicas, Información Jurídica, Legislación Federal Texto vigente al 30 de noviembre de 2005, [En línea]. Disponible: http://info4.juridicas.unam.mx, 15 abril de 2006.

- Señala que un certificado digital vigente, garantiza la autoría del documento digital como la autenticidad de su contenido, así como las reglas para su utilización.

- Señala que la firma electrónica avanzada, debe estar amparada por un certificado digital vigente, a fin de surtir los mismos efectos que los documentos con firma autógrafa.

- Define al documento digital como todo mensaje de datos que contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología.

- Se determina que los datos de identidad obtenidos por el SAT, para el trámite del certificado que ampare la firma electrónica avanzada, no quedan comprendidos dentro del secreto fiscal.

- Definir el concepto de sello digital que es el mensaje electrónico que acredita que un documento digital fue recibido por la autoridad correspondiente y estará sujeto a la misma regulación aplicable al uso de una firma electrónica avanzada. En este caso, el sello digital identificará a la dependencia que recibió el documento y se presumirá, salvo prueba en contrario, que el documento digital fue recibido en la hora y fecha que se consignen en el acuse de recibo mencionado.

- Otorga al SAT facultades para proporcionar los servicios de firma electrónica avanzada:

- Da los requisitos para ser considerados válidos los certificados, así como los supuestos en que quedarán sin efectos los certificados emitidos por el SAT;

- Precisa que la integridad y autoría de un documento digital con firma electrónica avanzada o sello digital sea verificable mediante el método de remisión al documento original con la clave pública del autor;

- Y señala las obligaciones del titular de un certificado emitido por el SAT.

2.2.7 Ley Federal de Protección al Consumidor

En la multicitada reforma de 2000, también se modificaron algunos artículos de la ley Federal de Protección al Consumidor, en cuanto a la relación que guardan los medios electrónicos y los consumidores, como a continuación se destaca:

> **". . . ARTÍCULO CUARTO.-** Se reforma el párrafo primero del artículo 128, y se adiciona la fracción VIII al artículo 1º la fracción IX bis al artículo 24 y el Capítulo VIII bis a la Ley Federal de Protección al consumidor que contendrá el artículo 76 bis para quedar como sigue":
>
> **Artículo 1º.-** . . . I a VII
>
> **VIII.-** La efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los medios aportados.
>
> **Artículo 24.-** . . . I a IX
>
> **IX bis.-** Promover en coordinación con la Secretaría la formulación, difusión y uso de códigos de ética, por parte de proveedores que incorporen los principios previstos por esta Ley respecto de las

transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

CAPÍTULO VIII BIS

DE LOS DERECHOS DE LOS CONSUMIDORES EN LAS TRANSACCIONES EFECTUADAS A TRAVÉS DEL USO DE MEDIOS ELECTRÓNICOS, ÓPTICOS O DE CUALQUIER OTRA TECNOLOGÍA

ARTÍCULO 76 bis.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente.

I.- El proveedor utilizara la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;

II.- El proveedor utilizara alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor informara a este previamente a la celebración de la transacción de las características generales de dichos elementos;

III.- El proveedor deberá proporcionar al consumidor antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;

IV.- El proveedor evitara las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes que ofrezca, señaladas en esta Ley y de más disposiciones que se deriven de ella;

V.- El consumidor tendrá derecho a conocer toda la información sobre los términos condiciones, costos, cargos adicionales en su caso formas de pago de los bienes y servicios ofrecidos por el proveedor;

VI. El proveedor respetara la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y

VII.- El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y cuidara las practicas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población. . . . .”

En esta reforma se destaca:

- Reconoce como relaciones comerciales las realizadas por medios electrónicos;

- Trata de evitar actos fraudulentos estableciendo las obligaciones de los proveedores, como la manera confidencial en que debe de manejar la información que le sea proporcionada por el usuario;

- El proveedor debe proporcionar antes de cualquier operación su domicilio, números etc., en fin todos y cada uno de los datos necesarios para su identificación en caso de una posible reclamación;

- Proteger los derechos de los consumidores que establezcan relaciones comerciales por medios electrónicos;

- Aunado a lo anterior la publicidad usada por el proveedor debe ser clara sobre los servicios que se ofrecen;

En esta misma reforma se omite mencionar lo siguiente:

- No establece como impondrá multa cuando el proveedor de los servicios es extranjero, tomando en cuenta que tal vez en su país no se ha legislado en materia electrónica, y en caso de haberse legislado el proveedor se acogerá a las leyes de su país;

- No menciona como es que un proveedor puede o no evitar practicas engañosas;

- En algunos casos la identificación y el domicilio del proveedor no se encuentran planamente comprobados, en este caso el usuario debe tomar las medidas necesarias para no hacer uso de esos sitios electrónicos;

- No establece la responsabilidad de los intermediarios, solo la considera entre usuario y proveedor;

2.2.8 Reglas para el Registro Público de Comercio

En la misma reforma de 2000, dentro de las modificaciones realizadas al Código de Comercio, existen algunas que están vinculadas a la forma en que el

Registro inscribirá las operaciones en materia mercantil; el modo en que se plantean los lineamientos para la operación y las formas para llevar acabo las inscripciones en el Registro Público de Comercio se encuentran contenidas en los acuerdos publicados en el Diario Oficial de la Federación del 18 de septiembre de 2000 pero estas las trataremos en el último capítulo de este trabajo, por lo pronto examinaremos el texto de la reforma de 2000 el cual establece:

> **"Artículo 18. -** En el Registro Público de comercio se inscriben los actos mercantiles, así como aquellos que se relacionan con los comerciantes y que conforme a la legislación lo requieran. La operación del Registro Público de Comercio esta a cargo de la Secretaría de Comercio y Fomento Industrial, en adelante la secretaria y de las autoridades responsables del registro público de la propiedad en los estados y en el Distrito Federal en términos de este código y de los convenios de coordinación que se suscriban conforme a lo dispuesto por el artículo 116 de la Constitución política de los Estados Unidos Mexicanos. Para estos efectos existirán las oficinas del Registro Público de Comercio en cada entidad federativa que demande él trafico mercantil. La Secretaria emitirá los lineamientos necesarios para la adecuada operación del Registro Público de comercio, que deberán publicarse en de Diario Oficial de la Federación.
>
> **Artículo 20.-** El registro público de comercio operara con un programa informático y con una base de datos central interconectada con las bases de datos de sus oficinas ubicadas en las entidades federativas, las bases de datos contaran con al menos un respaldo electrónico.

Mediante el programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral. Las bases de datos del Registro Público de Comercio en las entidades federativas se integraran con el conjunto de la información incorporada por medio del programa informático de cada inscripción o anotación de los actos mercantiles inscribibles, y la base de datos central con la información que los responsables del Registro incorporen en las bases de datos ubicadas en las entidades federativas. El programa informático será establecido por la secretaria. Dicho programa y las bases de datos del Registro Público de Comercio, serán propiedad del Gobierno Federal. En caso desistir discrepancia o presunción de alteración de la información del Registro Público de Comercio contenida en la base de datos de alguna entidad federativa o sobre cualquier otro respaldo que hubiere, prevalecerá la información registrada en la base de datos central, salvo prueba en contrario. La Secretaria establecerá los formatos, que serán de libre reproducción, así como los datos, requisitos y demás información necesaria para llevar a cabo las inscripciones, anotaciones y avisos a que se refiere el presente capítulo. Lo anterior deberá publicarse en le Diario oficial de la Federación.

Artículo 20 bis.- Los responsables de las oficinas del Registro Público de Comercio tendrán las atribuciones siguientes:

I.- Aplicar las disposiciones del presente capítulo en el ámbito de la entidad federativa correspondiente.

II.- Ser depositario de la fe pública registral mercantil, para cuyo ejercicio se auxiliara de los registradores de la oficina a su cargo;

III.- Dirigir y coordinar las funciones y actividades de las unidades administrativas a su cargo para que cumplan con lo previsto en este Código, el reglamento respectivo y los lineamientos que emita la Secretaria;

IV. Permitir la consulta de los asientos regístrales que obren en el Registro, así como expedir las certificaciones que le soliciten;

V. Operar el programa informático del sistema registral automatizado en la oficina a su cargo conforme a lo previsto en este Capítulo, el reglamento respectivo y en los lineamientos que emita la Secretaría;

VI. Proporcionar facilidades a la secretaria para vigilar la adecuada operación del Registro Público de Comercio;

VII. Las demás que señalen en el presente Capítulo y su reglamento.

Artículo 21.- Existirá un folio electrónico por cada comerciante o sociedad, en el que se anotaran: I a XIX

Artículo 21 bis.- El procedimiento para la inscripción de actos mercantiles en el Registro Público de Comercio se sujetara a las bases siguientes:

I. Será automatizado y estará sujeto a plazos máximos de respuesta;

II. Constara de las fases de: **a)** Recepción física o electrónica de una forma pre-codificada, acompañada del instrumento en el que conste el acto a inscribir, pago de los derechos, generación de una boleta de ingreso y del numero de control progresivo e invariable para cada acto;

b) Análisis de la forma precodificada y la verificación de la existencia o inexistencia de antecedentes regístrales y, en su caso, preinscripción de dicha información a la base de datos ubicada en la entidad federativa; **c)** Calificación en la que se autorizara en definitiva la inscripción en la base de datos mediante la firma electrónica del servidor público competente, con lo cual se generara o adicionara el folio mercantil electrónico correspondiente, y **d)** Emisión de una boleta de inscripción que será entregada física o electrónicamente. El reglamento del presente Capítulo desarrollara el procedimiento registral de acuerdo con las bases anteriores.

Artículo 21 bis 1.- La prelación entre derechos sobre dos o más actos que se refieran a un mismo folio mercantil electrónico, se determinara por él numero de control que otorgue el registro, cualquiera que sea la fecha de su constitución o celebración.

Artículo 22.- Cuando conforme a la ley, algún acto o contrato deba inscribirse en el Registro Público de la propiedad o en registros espéciales, su inscripción en dichos registros será bastante para que surtan los efectos correspondientes del derecho mercantil, siempre y cuando en el Registro Público de Comercio se tome razón de dicha inscripción y de las modificaciones a la misma.

Artículo 23.- Las inscripciones deberán hacerse en la oficina del Registro Público de Comercio del domicilio del comerciante pero si se trata de bienes o derechos reales constituidos sobre ellos, la inscripción

se hará, además en la oficina correspondiente a la ubicación de los bienes, salvo disposición legal que establezca otro procedimiento.

Artículo 24.- Las sociedades extranjeras deberán acreditar, para su inscripción en el Registro Público de Comercio, estar constituidas conforme a las leyes de su país de origen y autorizadas para ejercer el comercio por la secretaria, sin perjuicio de lo establecido en los tratados y convenios internacionales.

Artículo 25.- Los actos que conforme a este Código u otras leyes deban inscribirse en el Registro Público de comercio deberán constar en:

I. Instrumentos públicos otorgados ante notario o corredor público;

II. Resoluciones y providencias judiciales o administrativas certificadas;

III.- Documentos privados ratificados ante notario o corredor público o autoridad judicial competente según corresponda; o

IV. Los demás documentos que de conformidad con otras leyes así lo prevean.

Artículo 26.- Los documentos de procedencia extranjera que se refieran a actos inscribibles podrán constar previamente en instrumento público otorgado ante notario o corredor público para su inscripción en el Registro Público de Comercio. Las sentencias dictadas en el extranjero solo se registraran cuando medie orden de autoridad judicial mexicana competente, y de conformidad con las disposiciones internacionales aplicables.

Artículo 27.- La falta de Registro de los actos cuya inscripción sea obligatoria, hará que estos solo produzcan efectos jurídicos entre los

que lo celebren, y no podrán producir perjuicio a tercero él cual si podrá aprovecharse de ellos en lo que le fueren favorables.

Artículo 30.- Los particulares podrán consultar las bases de datos y en su caso, solicitar las certificaciones respectivas, previa pago de los derechos correspondientes. Las certificaciones se expedirán previa solicitud por escrito que deberá contener los datos que sean necesarios para la localización de los asientos sobre los que debe versar la certificación y, en su caso, la mención del folio mercantil electrónico correspondiente.

Cuando la solicitud respectiva haga referencia a actos aún no inscritos, pero ingresados a la oficina del registro Público de Comercio, las certificaciones se referirán a los asientos de presentación y tramite.

Artículo 30 bis.- La Secretaria podrá autorizar el acceso a la base de datos del registro Público de comercio a personas que así lo soliciten y cumplan con los requisitos para ello en los términos de este Capítulo, el reglamento respectivo y los lineamientos que emita la Secretaría, sin que dicha autorización implique en ningún caso inscribir o modificar los asientos regístrales. La Secretaría calificara los medios de identificación que utilicen las personas autorizadas para firmar electrónicamente la información relacionada con el Registro Público de Comercio, así como la de los demás usuarios del mismo, y ejercerá el control de estos medios a fin de salvaguardar la confidencialidad de la información que se remita por esta vía.

Artículo 30 bis.- Cuando la autorización a que se refiere él artículo anterior se otorgue a notarios o corredores públicos, dicha autorización permitirá, además, él envió de información por medios electrónicos al Registro y la remisión que este efectúe al fedatario público correspondiente del acuse que contenga él numero de control a que se refiere el artículo 21 bis de este Código. Los notarios y corredores públicos que lo soliciten dicha autorización deberá otorgar una fianza a favor de la Tesorería de la Federación y registrada ante la Secretaría, para garantizar los daños que pudieran ocasionar los particulares en la operación del programa informático por un monto mínimo equivalente a 10 000 veces el salario mínimo diario vigente en el Distrito Federal. En caso de que los notarios o corredores públicos estén obligados por la ley de la materia a garantizar el ejercicio de sus funciones, solo otorgaran la fianza a que se refiere el párrafo anterior por un monto equivalente a la diferencia entre esta y la otorgada. Dicha autorización y su cancelación deberán publicarse en el Diario Oficial de la Federación.

Artículo 31.- Los registradores no podrán denegar la inscripción de los documentos mercantiles que se les presenten salvo cuando:

I. El acto o contrato que en ellos se contenga no sea de los que deban inscribirse;

II. Este en manifiesta contradicción con los contenidos de los asientos regístrales preexistente;

III. El documento de que se trate no exprese o exprese sin claridad suficiente, los datos que deba contener la inscripción.

Si la autoridad administrativa o judicial ordena que se registre un instrumento rechazado la inscripción surtirá efectos desde que por primera vez se presento. El registrador suspenderá la inscripción de los actos a inscribir, siempre que existan defectos u omisiones que sean subsanables. En todo caso requerirá al interesado para que en el plazo que determine el reglamento de este Capítulo las subsane, en el entendido de que, de no hacerlo, se le denegara la inscripción.

Artículo 32.- La rectificación de los asientos en la base de datos por causa de error material o de concepto, solo procede cuando exista discrepancia entre el instrumento donde conste el acto y la inscripción. Se entenderá que se comete error material cuando se escriban unas palabras por otras, se omita la expresión de alguna circunstancia o se equivoquen los normes propios o las cantidades al copiarlas del instrumento donde conste el acto, sin cambiar por eso el sentido general de la inscripción ni el de alguno de sus conceptos. Se entenderá que se comete error de concepto cuando al expresar en la inscripción alguno d los contenidos del instrumento se altere o varíe su sentido por que el responsable de la inscripción se hubiere formado un juicio equivocado del mismo, por una errónea calificación del contrato o acto consignado o por cualquiera otra circunstancia similar.

Artículo 32 bis.- Cuando se trate de errores de concepto los asientos practicados en los folios del Registro Público de Comercio solo podrán rectificarse con el consentimiento de todos los interesados en le mismo asiento A falta del consentimiento unánime de los interesados, la

rectificación sólo podrá efectuarse por devolución judicial. El concepto rectificado surtirá efectos desde la fecha de su rectificación. El procedimiento para efectuar la rectificación en la base de datos lo determinara la Secretaría en los lineamientos que al efecto emitan.

Artículo 49.- Comerciantes están obligados a conservar por un plazo mínimo de 10 años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido integra e inalterada a partir del momento en que se genero por primera vez en si forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos".[91]

En esta reforma es destacarse:

- Se inscriben los actos comerciales y los que se relacionen con ellos, en folios electrónicos, lo anterior de acuerdo en que cada Estado de la República el Registro tendrá una oficina;

- El Registro operara con un programa informático con una base de datos central interconectada y con un respaldo electrónico.

[91] DIARIO OFICIAL DE LA FEDERACIÓN, op cit.

- Los responsables de las oficinas regístrales son depositarios de la fe pública registral mercantil;

- Establece las bases para inscribir los actos mercantiles dando importancia a la recepción física o electrónica de una forma pre-decodificada acompañada del instrumento en que conste el acto a inscribir, el pago de derechos lo que generara una boleta de ingreso y un numero de control; verifica que existan antecedentes regístrales; una vez lo anterior se autoriza la inscripción y se genera un folio mercantil y emite la boleta correspondiente;

- Contempla la prelación al momento de inscribir;

- Establece la inscripción hecha en el domicilio del comerciante o donde se encuentre el bien o derecho real;

- Las sociedades mercantiles extranjeras deben acreditar encontrarse constituidas y autorizadas para el comercio;

- Los actos que se pueden inscribir deben constar en instrumento público ante fedatario, la falta de inscripción sólo surte efectos entre las partes;

- Los particulares pueden consultar las bases de taos o solicitar certificaciones respectivas previo pago de derechos;

- La Secretaria autoriza acceso a la base de datos a las personas que lo soliciten;

- Cuando la autorización sea a notarios esta autorización permite él envió de la información por medios electrónicos al Registro y la remisión que este efectuó al fedatario del acuse que tiene él numero de control;

- Casi no hay casos en que el registrador pueda denegar la inscripción de algún acto;

- La rectificación de asientos por error solo procede cuando hay diferencia entre el instrumento donde conste el acto y la inscripción;

- Los errores de concepto, asientos practicados en los folios sólo su rectificación con consentimiento de interesados, si no la rectificación se tiene que hacer por devolución judicial.

Esta también omite:

- Como es que los particulares pueden consultar o solicitar las certificaciones respectivas, es decir, como se les proporcionara una clave para esto.

- Tomemos en cuenta que existen los hankers y que al entrar a la base de datos del Registro podrían hacer modificaciones que traerían consecuencias jurídicas.

CAPITULO III

DE LA FIRMA EN GENERAL

3.1 Concepto

3.2 Naturaleza y valor jurídico

3.3 Efectos jurídicos

3.4 Elementos formales

3.5 Características

3.6 Importancia

3.7 Clases de firmas
- 3.7.1 Firma en persona física y moral
- 3.7.2 Firma a ruego
- 3.7.3 Huella digital

3.8 Criptografía
- 3.8.1 Definición
- 3.8.2 Características
- 3.8.3 Clases de cifrado
  - 3.8.3.1 Criptografía simétrica
  - 3.8.3.2 Criptografía asimétrica
- 3.8.4 Propósitos por las que se cifran mensajes

CAPÍTULO III. DE LA FIRMA EN GENERAL

3.1 Concepto

Como ya se examino en el primer capítulo de este trabajo, desde los orígenes del hombre, este se comenzó a comunicar a través de signos que le eran únicos y con los cuáles identificaba sus pertenencias.

Otra forma por la que comenzó a comunicarse es por medio de la escritura y de la que podríamos decir que se deriva la firma, así que para llegar al concepto de firma como tal, señalaremos que la escritura es: "una técnica específica para fijar la actividad verbal mediante el uso de signos gráficos que representan ya sea iónica o bien convencionalmente la producción lingüística y que se realizan sobre la superficie de un material de características aptas para conseguir la finalidad básica de esta actividad que es dotar al mensaje de un cierto grado de durabilidad".[92]

Conforme a lo anterior, la escritura es un instrumento de comunicación que fue usada en sus orígenes como un requisito legal derivado de las transformaciones experimentadas por el propio Estado, el mercado comercial y la vida en sociedad.

Las primeras manifestaciones de la escritura se pueden ver en una gran variedad prácticas; ya sea como una forma en las que se puede dejar constancia de ciertas transacciones; o también en las peticiones presentadas ante

---

[92] TUSON, Jesús, *La escritura una introducción a la cultura alfabética*, Ediciones Octaedro S.L. España, 1997, págs 14 a 24.

autoridades; e igualmente en los documentos válidados por la intervención de un notario.

Me parece que la firma es una derivación de la manera en que cada persona escribe, ya que la firma y la escritura contienen rasgos similares que permiten vincular a la persona que escribió y que firmó un documento.

Ahora bien el concepto de firma digital que analizaremos más adelante, rompe con el esquema jurídico tradicional de manifestar nuestra voluntad en los contratos que se presentan por escrito, y aunque el tema central de este trabajo es la firma digital, tendremos primeramente que analizar el concepto de la firma tradicional o manuscrita.

La palabra "firma" proviene del latín firmare, lo que significa afirmar, corroborar, confirmar, dar fuerza al contenido de un documento, ligado a esto la palabra "autógrafa" significa grabar o escribir por sí mismo y se aplica al escrito de mano de su propio autor, pero bien entendido que los signos o trazos han de ser hechos por la mano del autor sin que la impresión se haga por medios mecánicos.[93]

El Diccionario de la Real Academia Española define a la firma como "el nombre y apellido o título de una persona, que esta pone su rúbrica al pie del documento escrito de mano propia o ajena para darle autenticidad y para expresar que se aprueba su contenido o para obligarse a lo que en él se dice" [94]

En el Vocabulario Jurídico de Couture se define a la firma como "un trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de

[93] ENCICLOPEDIA JURÍDICA OMEBA, op cit, págs 290-293.
[94] DICCIONARIO DE LA REAL ACADEMIA DE LA LENGUA ESPAÑOLA, Vigésima Edición, Tomo I, Editorial Espasa Calpe, España, 1990, p 88.

una persona, con el cuál se suscriben los documentos para darles autoría virtualidad y obligarse en lo que ellos se dicen"[95]

Por otra parte Tullio Ascarelli indica que "la firma debe inscribirse toda por él emítete o girador (refiriéndose a la materia mercantil) con pluma o lápiz con buena o mala caligrafía debe contener el nombre y el apellido o el nombre comercial del suscriptor con la firma relativa, también puede limitarse al solo apellido con la inicial, del nombre o su abreviatura"[96]

En materia bancaria Miguel Acosta Romero indica que se debe entender a la firma autógrafa como "la que suscribe una persona física con su propia mano y consiste en un conjunto de letras o bien algún componente de su nombre y a veces el nombre y apellidos, aunado a una serie de trazos caprichosos que pudieran abarcar toda gama de evoluciones de instrumento de escritura que señalan e identifican al sujeto y lo separan de otros en los documentos que suscribe y es un elemento que refleja permanentemente su voluntad de expresar lo que firma y de obligarse al tema del texto que suscribe"[97]

Por último Planiol y Ripert señala que la firma "es una inscripción manuscrita que indica el nombre de una persona que tiende hacer suyas las declaraciones del acto."

---

[95] COUTURE, Eduardo Juan, *Vocabulario Jurídico*, Editorial Depalma, Argentina, 1998, p 30.
[96] ASCARELLI, Tullio, *Derecho Mercantil Mexicano*, (DE J. TENA Felipe), 18ª edición, Editorial Porrua, México, 1999, p 46.
[97] ACOSTA ROMERO, Miguel, *Derecho Bancario, panorama del sistema financiero mexicano*, 4ª edición, Editorial Porrua, México 1991, p 251.

Y Mustapich también la define como “el nombre escrito por propia mano de caracteres alfabéticos y de una manera particular al pie del documento, al efecto de autenticar su contenido”[98]

Podemos observar que en la actualidad ambas definiciones, no concuerdan con la realidad ya que en la primera de ellas al decir que la firma “. . . indica el nombre de una persona. . . ”; y en la segunda al indicar que “. . . la firma es el nombre escrito por propia mano en caracteres alfabéticos . . .”; si siguiéramos ambas definiciones estas dejarían sin efecto aquellas firmas que se componen solo de trazos que no sólo expresan el nombre del firmante sino que se componen de rasgos no asimilables a caracteres alfabéticos; ahora ambas definiciones si coinciden en señalar 2 constantes que deben de prevalecer para que la firma sea tomada como tal, en primer término el hecho de tratarse de una inscripción manuscrita realizada de una manera particular y en segundo término el que dicha inscripción sea hecha con el ánimo de obligarse al reconocimiento del contexto del escrito en que se haga.

Ya con las anteriores definiciones, podemos ver que la mayoría de los autores coinciden en que la firma es el signo distintivo de la persona jurídica que lo estampa y que para que la firma tenga el valor jurídico que más adelante trataremos, esta debe contener la inscripción manuscrita puesta en forma particular de la persona que va a suscribir el documento ya que dicha firma debe ser estampada con él ánimo de obligarse y de indicar su consentimiento expreso con las manifestaciones que se encuentran dentro del documento que el firmante aprueba estos signos pueden ser desde un mero monosílabo hasta el más

[98] ENCICLOPEDIA JURÍDICA OMEBA, op cit, págs 290-293.

complicado complementación de caracteres alfabéticos que individualiza al ser humano.

3.2 Naturaleza y valor jurídico de la firma

Ya con lo mencionado podemos decir que la naturaleza jurídica de la firma radica en la afirmación de la individualidad entendiendo por esto plasmar la voluntad de él que firma ya que en primer lugar significa que ha sido la persona firmante y no otra quien suscribió el documento y el segundo lugar que la persona firmante acepta lo que ahí se manifestó, como vemos a lo que aludimos antes son aspectos que constituyen el porque de la existencia de la firma; el por que fue creada y como se fundamenta su uso como un instrumento legal sobre la aceptación o afirmación del instrumento que la contiene.

Aún conociendo las diversas definiciones que existen sobre la firma, sabemos que en los numerosos cuerpos normativos en nuestro país, prácticamente no hay una definición de la firma autógrafa o simplemente de la firma en general y mucho menos se trata a esta como un requisito de autenticidad o sine cuan non, ya que en muchos de ellos solo dice que el documento deberá estar firmado para tal o cuál acto jurídico, pero no va más allá de su mención aunque desde el punto de vista legal se le ha asignado un valor jurídico a las distintas representaciones de esta autenticación o confirmación de la identidad de la persona.

Para entender mejor la naturaleza y el valor jurídico de una firma, tenemos que analizarla desde 2 puntos de vista:

a) Primero como un acto jurídico, la firma es consecuencia de un proceso que pasa de percepciones externas a lo material es decir primero la persona analiza y procesa de alguna manera la información, lo que le permite determinar si esta de acuerdo o no, por lo que su conclusión o decisión la refleja físicamente interviniendo en ello su voluntad, y dando como resultado final de tal proceso mental, que el individuo firme y en consecuencia adquiriendo entonces trascendencia jurídica;

b) Segundo como una forma de exteriorizar la voluntad, se sabe que la voluntad es lo que impulsa al hombre a hacer o no hacer determinada cosa, en cuanto a la firma para determinar si esta fue plasmada como consecuencia de un acto voluntario y de acuerdo al proceso del que hablamos en el punto anterior diremos que al firmar y exteriorizar nuestra voluntad interviene en ellos la concepción que se genera de forma autónoma donde solo el que suscribe la procesa internamente; la representación que una vez superado la concepción se genera la forma en que una persona se va a expresar y como es que va a representar lo que quiere plasmar; la decisión donde se delibera sobre lo que se desea hacer y por último la ejecución donde se materializa la voluntada físicamente, por medio de signos individuales lo que significa que una vez plasmada la firma sé esta dé acuerdo con el documento lo cuál es el objeto de la voluntad exterioriza generando además derechos y obligaciones por lo tanto loa voluntad y el objeto conjuntados hacen que la firma tenga válidez jurídica.[99]

---

[99] GAETE GONZÁLEZ, Eugenio Alberto, *Instrumento Público Electrónico*, 2ª Edición, Editorial Bosch S.A., España 2002, págs 111 – 133.

3.3 Efectos Jurídicos

En cuanto a los efectos jurídicos de la firma se debe de considerar la naturaleza del documento donde aparece una firma ya que se puede firmar tanto para dar fe pública, autenticar documentos o ratificarlos; tal es el caso de los notarios públicos que al dar fe o autenticar un acto hacen que este produzca efectos jurídicos, ya que la firma de este fedatario, junto con otros elementos, como su sello hacen en si la fe pública mediante la que se formaliza, solemniza y autentifica actos jurídicos entre las partes y salvo la responsabilidad que puede derivarse por desempeño su función los derechos y obligaciones que se pudieran derivar del acto no las afecta.

3.4 Elementos formales

Estos están integrados por el conjunto de letras, palabras, frases signos de determinada inclinación y trayectoria que constituyen la forma física de la firma.

Como ya vimos en nuestra legislación no existe mención de los elementos formales que constituyen a la firma por lo tanto existe una cierta libertad para usar cualquier forma de firma; tratando en lo posible de que cada firma contenga los mismos rasgos para no dar lugar a controversias de ninguna naturaleza.

Ahora bien tampoco la legislación enuncia limitantes para firmar de tal o cuál manera, entonces una persona podría firmar plasmando solo su nombre y apellido, a las que les pueden a agregar rasgos, signos en cualquier dirección, siempre tratando que el signatario realice el mismo signo.

En algunos casos pueden existir firmas que pueden ser totalmente legibles o ilegibles, en cuanto a las primeras diremos que se componen de signos que se pueden identificar plenamente por ejemplo por el nombre y apellido, a los que agregan ciertos rasgos y en ocasiones también pueden tener rúbrica; sin embargo en cuanto a las segundas estas solo constan de rasgos que no contienen alguna letra y que pueden llegar a ser verdaderos escritos difíciles de descifrar; en ambos casos es posible poder conocer con certeza a quien pertenece una firma ya sea por que sea cotejada con otra o en caso necesario por estudios de caligrafía o de peritos así que para los efectos de válidez jurídicos ambos tipos tienen la misma consecuencia y nacen de la exteriorización de la voluntad.

3.5 Características

Ya mencionamos que la firma es una de las condiciones esenciales para que puedan existir los documentos y para que estos puedan surtir efectos frente a otras personas.

Haremos algunas consideraciones que nos permitan llegar a determinar las características de las que se conforma una firma:

a) Una firma estampada así sola en un documento no tiene el carácter de auténtica, pues para que sé de tal supuesto esta debe ser reconocida por la persona a quien la ley le atribuye la fe pública, o bien que sea declarada judicialmente entonces la primera característica es la: autenticidad.

b) Consideremos que a pesar que las personas tienen cierta libertad para escoger la forma con que van a firmar sus documentos y por consiguiente

autenticar los mismos están condicionados a que una vez que se ha elegido la forma de firmar esta ya no puede ser modificada a cada momento, así que el signo o trazo con el cual firma una persona es aquel con el que lo hace de manera ordinaria, más allá de estampar el mismo signo frecuentemente, esta es la intención del firmante de no variar su firma, así que la variación de una firma ayuda a determinar la veracidad de esta así que la segunda característica la llamaremos a la manera habitual del uso;

c) Aunado a lo anterior y como contraposición también sabemos y esta probado que nunca una firma es exactamente igual a la estampada con anterioridad, aunque haya sido firmada por la misma persona, así que otra de las características seria: irregularidad de las firmas;

d) Si tomamos en cuenta que cada una de las firmas existentes es propia de una persona y nada más es el modo particular que cada persona tiene para firmar un documento, es decir que la firma tiene rasgos, trazos o signos que son el modo particular que cada persona tiene para suscribir un documento; así que otra de las características es la: peculiaridad de cada persona para firmar;

e) Por último cada firma debe ser estampada de puño y letra por el firmante, y que implica la asunción del contenido del documento y manifestación de voluntad a lo consignado en el documento, aceptando el otorgamiento del acto, así que la última característica es que la firma debe ser: autógrafa.[100]

[100] REYES KRAFFT, Alfredo Alejandro, *Firma Electrónica y Entidades de Certificación*, 1ª Edición, Editorial Porrua México 2003, págs 159 y 160.

3.6 Importancia

La importancia de una firma radica en la autoría de un determinado documento, o sea, la persona que suscribe tal documento hace suyo el contenido y se obliga a lo que se establece en él.

La imposición de una firma produce el efecto de que el acto contenido en ese documento le sea imputado al firmante ya que este pretendería negar la autoría o la aceptación del documento a un lado de su firma tendría que demostrar por los medios que la ley establece.

Ahora bien una firma es importante por que además de lo antes dicho en el párrafo anterior esta sirve para:

a) Expresar consentimiento sobre o la intención de asignarle efectos jurídicos;

Ya vimos que desde la edad media la declaración escrita sé hacia poniendo el nombre propio de bajo de un acto escrito, así la firma establece la voluntad de que firma;

b) Para investir de solemnidad un acto ya que el hecho de firmar un documento llama a la reflexión a la que firma respecto del acto jurídico;

En consecuencia la solemnidad tiende a evitar la asunción de compromisos de una manera inconsciente.

c) En el tema que nos ocupa una firma sirve para dar autenticidad al cuerpo de una escritura que le precede al autentificar al signatario;

Cuando el que firma coloca al pie de un documento un signo que lo caracteriza la escritura se vuelve atribuible a él.

d) A veces la firma hace la validez de los actos jurídicos que se celebran es decir la firma es una condición esencial para la existencia de todo acto bajo la forma privada.[101]

3.7 Clases de firmas

3.7.1 Firma en persona física y moral

Es obvio que cualquier firma estampada por un individuo, aunque habría que hacer una deferencia entre una persona física y una moral ya que la calidad con que concurre cada una de ellas al acto jurídico es diferente, es decir ya que una actúa por nombre propio y la otra en representación de.

La persona física, es la que firma un documento a nombre propio es decir firma por su propio derecho, sin ninguna clase de representación, asumiendo desde luego que la forma en la que comparece, lo cuál producirá efectos jurídicos, es decir estará conciente el signatario del alcance legar que su firma llegare a tener.

En pocas palabras la persona física es quien va a dejar constancia de la realización de un acto, es decir materializará su consentimiento o voluntad por medio de la firma.

En el caso de la persona moral la calidad con la que comparece una persona es distinta, ya que comparece a firmar un documento en nombre y

[101] VIVIANA SARRA Andrea, *Comercio Electrónico y Derecho*, Editorial Astrea, Argentina, 2000, p 167.

representación de una entidad moral, como representante legal apoderado o prestando servicio a una entidad pública, y aunque es una persona física quien firma esta queda acreditada a través de un nombramiento o poder, cuando esta actúa en su nombre y representación obliga a la persona moral produciendo efectos jurídicos, por lo tanto quedando obligada frente a terceros, y aunque sabemos que la representación es donde se concentra la dirección o gestión propia de la persona moral, esta también quien establece los limites y facultades de quien los representan lo que podemos ver que se establece en el Código Civil del Distrito Federal, en su Titulo Segundo que trata de las Personas Morales.

Entendamos como persona moral, al estado, una asociación o sociedad mercantil, con personalidad jurídica propia y con los mismos atributos a los que tendría una persona física; también tendría los mismos derechos y obligaciones ya que la persona moral se obliga por conducto de los órganos que la representan, según disposición legal y conforme a sus escrituras constitutivas o de los acuerdos a que se llegue en sus asambleas generales.

Una persona moral tiene casi la misma naturaleza que una persona física es decir también tiene derecho de un nombre " . . . y tienen la voluntad propia distinta de la de sus socios, que no es la voluntad de uno solo por que tampoco son muchas las voluntades, las voluntades de todo poderdante esa voluntad es una voluntad social pero necesariamente es humana por el sustrato humano del propio ente colectrivo"[102]

[102] GRACIA DOMÍNGUEZ, Miguel Ángel. *Derecho Penal Fiscal, Las infracciones y multas fiscales*, Editorial Porrua, México, 1994, págs 145 a 150.

3.7.2 Firma a Ruego

Al encontrarnos en el supuesto de que alguna persona no sepa firmar, en ocasiones por analfabetismo y otras por algún impedimento físico es cuando aparece en el ámbito del derecho la firma a ruego y a la huella digital estudiemos ambas entendiendo primero la firma a ruego.

La firma ruego es una modalidad que se aplica en el derecho, a los instrumentos públicos ". . . la firma a ruego consiste en la posibilidad de que otra persona distinta en principio de las partes suscriba el documento a petición o instancia de aquélla que no sabe o no puede escribir. El rogado firma pues el instrumento público en defecto de la parte que por un impedimento de tipo permanente o de carácter transitorio. . . no puede firmar por sí misma"[103]

Carlos E. González en su libro Teoría General del instrumento público, citado en la Enciclopedia Jurídica Omeba definen a la firma a ruego expresando que es la que hace una persona ajena al acto o negocio instrumentando colocando su propia firma a pedido del imposibilitado que es parte inetrveniente.[104]

De acuerdo a la anterior definición al decir "persona ajena al acto" es controvertido ya que la ley establece que para dar seguridad de que el documento cubre el requisito de ser firmado por el interesado, pero de ninguna manera ofrece la garantía de igualdad entre las partes puesto que el acto se realiza de buena fe.

Por eso se prevé que para quienes en algún momento deben obligarse y no saben leer ni escribir, lo hagan a través de la impresión de su huella digital o

---

[103] Ídem.
[104] Ídem.

pedir a una persona en quien confiere que si sabe escribir lo haga, reunidos estos elementos la firma alcanza fuerza legal.

En legislaciones como la Argentina para que se pueda hacer uso de la firma a ruego, se necesita que se den ciertos supuestos de derecho civil:

a) Que se trate de un instrumento público, ya que la Ley no autoriza la firma a ruego en un instrumento privado, requiriendo como condición para la existencia de tales actos la firma de las partes en sus propios nombres;

b) Que una o alguna de las partes no sepa o no pueda firmar;

c) Que otra persona distinta de la impedida o imposibilitada firme por esta a su instancia y solicitud

d) Que la persona del rogado no sea testigo instrumental"[105]

La legislación Argentina establece la fuerza probatoria de un documento firmado a ruego, se da cuando en ello interviene un depositario de la fe pública.

En nuestra legislación civil se acepta la firma a ruego, que consiste en la impresión de la huella digital, del obligado en el documento o parte del contrato firmando otra persona a su ruego y encargo cuando no sabe o no puede firmar; la huella digital acompañada de la firma a su nombre y ruego alcanza válidez pero queda la duda si el obligado en el documento conoce a plenitud el alcance del compromiso que asume.

Por eso se prevé que para quienes en algún momento deben obligarse y no saben leer ni escribir lo hagan a través e la impresión de su huella digital o pedir a otra persona en quien confié que si sabe leer y escribir lo haga, reunidos estos elementos la firma alcanza fuerza legal.

---

[105] Ídem.

3.7.3 Huella digital

La ciencia que hace el estudio de la impresión digital es la dactiloscopia que etimológicamente significa examen de los dedos, las huellas digitales son la identidad del hombre; así que la huella digital es la impresión de las líneas o yemas de los dedos de las manos de las personas físicas en cualquier objeto.[106]

Podemos decir que la huella digital es el mejor medio de identificación que existe de cada persona ya que las huellas de un individuo no son iguales a las de otro individuo.

En la legislación de nuestro país se permite en casos de excepción que las huellas dactilares impresas de las personas se tengan como medio de exteriorizar su voluntad para distintos actos jurídicos.

Con la impresión de la huella digital en el caso de quienes no saben leer ni escribir, la huella establece su presencia pero no su decisión o consentimiento ya que no queda plenamente enterado del alcance y contenido del documento con el que sé esta comprometiendo, por eso la legislación mexicana en general ha establecido que otra persona sea la que firme a su ruego.

La huella digital solo prueba presencia de la persona de cuya persona imprime la huella pero no es su voluntad.

Por último la huella digital no suple la falta del interesado pues si bien la impresión de la huella es señal inequívoca de identificación y por tanto de la certeza con respecto a la persona que la estampa no es una prueba de voluntad

---

[106] NANDO LEFORT, Víctor, *Diccionario Terminológico de Ciencias Forenses*, Editorial Trillas, México 1998, p 26.

pues quien si lo hace generalmente no sabe leer ni escribir, por lo tanto la ley no puede tener efecto sobre esas declaraciones por lo que se dice que la firma tiene ojos y voluntad y la huella en cierta forma es ciega.

3.8 Criptografía

A pesar de los numerosos avances tecnológicos que existen hoy en día en la forma en que podemos comunicarnos, se sabe que algunos de ellos no suelen ser tan seguros como quisiéramos, ya que existen ciertos riesgos, al enviar información con otra persona a través de cualquier medio tecnológico, la información enviada por la Internet no garantiza que los datos intercambiados entre dos o más personas, este libre de alteración o de que alguien ajeno pueda tener acceso a ellos, es por eso que para dar un sentimiento de seguridad y confidencialidad en operaciones o intercambio de información a través de la red se han desarrollado diferentes técnicas para lógralo, una de esas técnicas es la denominada: Criptografía.

3.8.1 Definición

Podríamos decir que desde el antiguo Egipto a la era digital ya se usaban mensajes cifrados para intercambiar información que era considerada altamente confidencial o sensible.

Aunque en cierta forma el sistema de jeroglíficos egipcio puede considerarse ya una forma de criptografía, el primer sistema criptográfico como tal

conocido de debe a Julio César. Su sistema consistía en reemplazar en el mensaje a enviar cada letra por las situadas tres posiciones por delante en el alfabeto latino.[107]

La palabra cifrar significa "trasformar una información (texto claro) en otra inteligible (texto cifrado o criptograma) según un procedimiento y usando una clave determinada pretendiendo que solo quien conoce dicho procedimiento (algoritmo de encriptación) y clave puede acceder a la información original. La operación inversa de llama descifrar".[108]

La ciencia que estudia, la ocultación, disimulación y el cifrado de la información, así como el diseñar sistemas que hagan estas funciones es la criptología; la cuál abarca a la criptografía (datos y texto), la criptofonía (voz) y criptoanálisis que es la ciencia que estudia los pasos y operaciones orientadas a trasformar un criptosistema en el texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y la clave; algunos autores definen a la criptografía como "la ciencia que se ocupa de trasformar mensaje en formas aparentemente inteligibles y devolverlos a su forma original.[109]

Otros la definen como "una escritura cifrada según una determinada clave que es necesario conocer para interpretar el mensaje, así encriptar un mensaje, es asignar códigos secretos y cifrados para proteger información mediante técnicas de criptografía de manera tal que el mensaje no tenga sentido mientras sé esta

---

[107] Wikipedia, Enciclopedia Libre, Criptografía, 28 marzo 2006, [En línea]. Disponible: http://es.wikipedia.org/wiki/Criptograf%C3%ADa, 14 abril de 2006.

[108] El Rincón de Quevedo. Criptografía. [En línea]. Disponible: http://www.rinconquevedo.iespana.es/rinconquevedo/Criptografia/rsa2000.htm, 14 abril de 2006.

[109] MARTÍNEZ NADAL, Apol-Lonia, *Comercio Electrónico, Firma Digital y Autoridades de Certificación*, 3ª Edición, Editorial Civitas, España, 2001, p 45.

transmitiendo y solo pueda ser decodificado o descifrado cuando llegue a su destino.[110]

La criptografía, de acuerdo con la Real Academia Española, proviene del griego “kryptos” que significa escondido y “graphein” que significa escribir y se podría decir que es el arte de enmascarar mensajes con signos normales que solo tienen sentido a la luz de una clave secreta por lo tanto, es la técnica de escribir con claves secretas o de un modo enigmático. En informática se define como “el arte y la ciencia de mantener seguros archivos y mensajes”. Se usan los términos codificar y descodificar; cifrar y descifrar como sinónimos de encriptar y/ desencriptar.[111]

De acuerdo a las definiciones anteriores diremos que la criptografía (encriptar)[112] como tal y su uso sería el remedio a la incertidumbre de que la información que estamos enviando y recibiendo a través de la red, es la que originalmente se generó.

3.8.2 Características

Varias son las características que deben de cubrir la transferencia de datos a través de la red y que podrían definir una comunicación como segura:

---

[110] Ídem.
[111] DICCIONARIO DE LA REAL ACADEMIA DE LA LENGUA ESPAÑOLA, op cit, p 50.
[112] Encriptar “es un sinónimo de la criptografía, ya que el encriptado de información se hace mediante una clave simétrica o secreto compartido o también por una clave asimétrica o esquema de clave pública sin las cuales la información no puede ser descifrada. La encriptación al igual que la criptografía es un conjunto de técnicas que intentan hacer inaccesible información a personas no autorizadas, el encriptar datos tiene los mismos objetivos que la criptografía es decir, la confidencialidad, para mantener la información en secreto, y la integridad, para evitar que la información se destruya. MORENO MARTÍN, Arturo, *Diccionario de Informática y telecomunicaciones*, Editorial Ariel, España 2001, p 22.

a) Confidencialidad: implica que la información está oculta para cualquiera que no sean las partes autorizadas a verla. Para proveer confidencialidad a la información la misma debe ser encriptada.

b) Se debe tener en cuenta que existen dos casos diferentes: cuando los datos son transmitidos o cuando son almacenados. En el primer caso las claves que permiten encriptar o desencriptar deben cambiar periódicamente y no deben ser guardadas, mientras que en el segundo caso es importante almacenarlas en forma protegida.

c) Integridad: implica que la información no sea alterada por partes no autorizadas, tanto durante la transmisión como durante el almacenamiento.

d) No-Repudio: implica que el emisor no pueda negar la emisión del mensaje.

e) No-Reenvío: implica que una información o mensaje no pueda ser reenviado por alguien que ha capturado una transacción legal.

f) Autenticación o Autenticidad: implica probar la identidad de una parte a otra. Esta provee que alguien no pueda falsear su propia identidad, y permite que el receptor determine fehacientemente la identidad del emisor."[113]

Para entender los conceptos antes trascritos partamos de que en el intercambio de información participan A como quien envía (emisor) el mensaje y B como el que recibe (receptor).

Veamos primero que la confidencialidad se trata de la seguridad de que los datos que contiene un documento están ocultos a ojos de terceras personas,

---

[113] Seguri Data, SeguriDoc, Integridad, autenticidad, no repudio de origen y confidencialidad para sus archivos, [En línea]. Disponible: http://www.seguridata.com/Brochure SeguriDoc.pdf, 14 abril de 2006.

aquí se toma en cuenta que se hace con los datos una vez que han llegado a su destinatario final, ya que la información que recibe este debe ser almacenada con todo cuidado, una agresión a la confidencialidad seria la captura del documento en su viaje de A hacia B y el uso indebido de los datos que sean almacenados por parte de B, la confidencialidad se consigue por medios criptográficos.

La integridad consiste en la seguridad de que los datos del documento enviado desde A hacia B, no sufrió modificación alguna a lo largo del viaje, una trasgresión a este punto seria si una tercera persona capturara el documento en su camino, la comprobación de la integridad se realiza mediante firmas electrónicas basadas en funciones denominadas hash, que veremos más adelante.

El no repudió es que una vez enviado el documento por A este no puede negar su autoría, como por ejemplo si alguien entrara a una subasta por Internet, y después no sostuviera su ofrecimiento, no podría repudiar que él generó la oferta basándose en esta característica.

El no reenvió de la información se denomina a que una vez, que se realizó una transacción legal, y alguien ajeno a dicha negociación recibe información por error este no reenvíe la información para confirmar o negar algo, lo que tendría que hacer es informar que esta recibiendo información por error.

Por último en cuanto a la autenticación imaginemos que B recibe un documento de A, como sabemos que realmente ambas personas son quien dicen ser, para dar autenticidad al documento tiene que contener una firma digital, basada en la criptografía.

De lo anterior podemos deducir que la autenticidad es una condición suficiente para la integridad, por lo tanto si un documento es autentico es integro, pero no al revés; e igualmente el no repudió es suficiente para la autenticidad, por lo que sí un documento es no repudiable es autentico, pero no al revés.

Cualquier sistema de transferencia de información que sea considerada como segura debe basarse en los puntos descritos antes, aunque algunos sistemas no contienen estos elementos.

3.8.3 Clases de cifrado

La criptografía funciona mediante el uso de un algoritmo matemático con el objeto de cifrar (codificar) datos para hacerlos incomprensibles para cualquier persona que no tenga una clave, es decir la información secreta necesaria para descifrar (decodificar) los datos codificados.[114]

Tradicionalmente la clave secreta era un clave compartida entre el emisor y el receptor llamada criptografía simétrica, hasta que se desarrollo la criptografía asimétrica, la que permite intercambiar datos cifrados sin que se tenga que intercambiar una clave que es secreta, por lo tanto en la criptografía coexisten dos claves una pública y una privada, cuyo significado esta implícito, diferentes pero relacionadas entre si; analicemos cada una de ellas.

Según Luciano Moreno, del departamento de diseño web de BJS Software (al cuál citaremos ampliamente por tratar el tema que nos ocupa de una

[114] LLANEZA GONZÁLEZ, Paloma, *Internet y comunicaciones digitales, Régimen legal de las tecnologías de la información y la comunicación,* Editorial Bosch, España 2000, p 297.

forma muy fácil y concreta), la forma de enviar información cifrada a través de la red se da principalmente por los siguientes factores:

a) Velocidad de cálculo: con la aparición de los computadores se dispuso de una potencia de cálculo muy superior a la de los métodos clásicos.

b) Avance de las matemáticas: que permitieron encontrar y definir con claridad sistemas criptográficos estables y seguros.

c) Necesidades de seguridad: surgieron muchas actividades nuevas que precisaban la ocultación de datos, con lo que la Criptología experimentó un fuerte avance".[115]

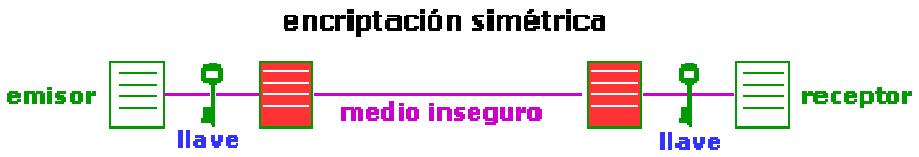
A partir de estas bases surgieron nuevos y complejos sistemas criptográficos, lo cual se materializa en dos métodos o clases: criptografía simétrica y la criptografía asimétrica.

3.8.3.1 Criptografía simétrica

También denominada de clave secreta, y se caracteriza por que se usa una misma clave para encriptar y para desencriptar, motivo por el que se denomina simétrica, veamos un cuadro que Luciano Moreno usa para ejemplificarla:

---

[115] MORENO, Luciano, *Manual de criptografía*, Departamento de diseño web BJS Software. [En línea]. Disponible: http://www.htm/web.net/seguridad/cripto/cripto_1.htm/, 14 abril de 2006.



"Toda la seguridad de este sistema está basada en la llave simétrica, por lo que es misión fundamental tanto del emisor como del receptor conocer esta clave y mantenerla en secreto. Si la llave cae en manos de terceros, el sistema deja de ser seguro, por lo que habría que desechar dicha llave y generar una nueva.

Para que un algoritmo de este tipo sea considerado fiable debe cumplir dos requisitos básicos:

a) Conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la clave.

b) Conocidos el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.

Generalmente el algoritmo de encriptación es conocido, se divulga públicamente, por lo que la fortaleza del mismo dependerá de su complejidad interna y sobre todo de la longitud de la clave empleada, ya que una de las formas de criptoanálisis primario de cualquier tipo de sistema es la de prueba-ensayo, mediante la que se van probando diferentes claves hasta encontrar la correcta.

Los algoritmos simétricos encriptan bloques de texto del documento original, y son más sencillos que los sistemas de clave pública, por lo que sus procesos de encriptación y desencriptación son más rápidos.

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, y los principales algoritmos simétricos actuales son **DES**, **IDEA** y **RC5**.[116]

Actualmente se está llevando a cabo un proceso de selección para establecer un sistema simétrico estándar, que se llamará **AES**[117] (Advanced Encryption Standart), que se quiere que sea el nuevo sistema que se adopte en el ámbito mundial".

Siguiendo la anterior en este sistema durante el proceso de cifrado y descifrado de un mensaje, las partes deben compartir una clave que les es común,

---

[116] Algoritmos: * **DES** (Data Encryption Standard) son esquemas de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EE.UU. en colaboración con la empresa IBM, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de ordenadores. Estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fue sometido a las leyes de USA. Se basa en un sistema mono alfabético, con un algoritmo de cifrado.
*** IDEA** es un sistema criptográfico simétrico, creado en 1990 por Lai y Massey, que trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits usando operaciones como OR-Exclusiva y suma y multiplicación de enteros. El algoritmo de desencriptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar, y hasta ahora no ha sido roto nunca, aportando su longitud de clave una seguridad fuerte ante los ataques. Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ampliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP.
*** RC5** usa una operación, llamada dependencia de datos, que aplica sifths a los datos para obtener así el mensaje cifrado. Ambos han sido creados por RSA Data Security Inc, empresa creada por los autores del sistema RSA, que es actualmente una de las más importantes en el campo de los sistemas de cifrado y protección de datos. Es ampliamente configurable, permitiendo fijar diferentes longitudes de clave, número de iteraciones y tamaño de los bloques a cifrar, por lo que le permite adaptarse a cualquier aplicación. Por ejemplo, este algoritmo es el usado por Nestcape para implementar su sistema de seguridad en comunicaciones SSL (Secure Socket Layer). Ídem.
[117] El NIST de EE.UU., en busca de un nuevo sistema de encriptación simétrico que reúna las características funcionales y de seguridad necesarias, en 1977 un concurso en el ámbito mundial, invitando a los desarrolladores de este tipo de sistemas a crear un algoritmo que pueda ser tomado como estándar; este nuevo sistema de llamará **AES** (Advanced Encryption Standard), y el algoritmo que utilice se denominará **AEA** (Advanced Encryption Algorithm). Ídem.

y que es usada por cada una de las partes, respectivamente para cifrar o descifrar un mensaje, esta clave se ha acordado previamente, la cuál debe ser secreta para evitar el acceso no autorizado a datos confidenciales.

Podríamos decir que la seguridad de este sistema reside en la protección que cada usuario de a la clave.

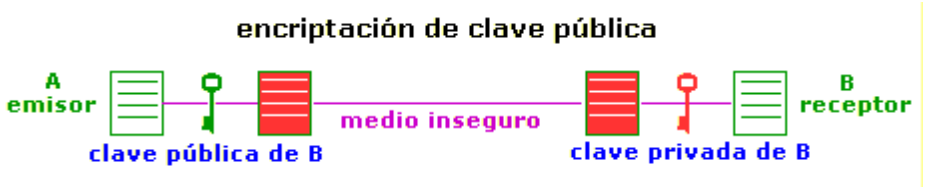
Aunque no creo que este sistema sea totalmente seguro si se pudiese decir que ofrece las características de confidencialidad, integridad y la autenticación.

Sin embargo este sistema también cuenta con inconvenientes, ya que la asignación de una clave se debe hacer a través de una red cerrada y totalmente confiable de lo contrario esta podría ser usada por una persona extraña que lograría interceptar información que solo incumbe a las partes; igualmente, como ya señalamos una de las características que cubre este sistema es la autenticación entre las partes, pero no lo cumple frente a terceros, ya que este tercero no podría determinar la autoría de un determinado mensaje; otra de las desventajas de este método es la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

Ahora bien en nuestra opinión este sistema no es tan completo ni ofrece tanta seguridad como un cifrado asimétrico, ya que aunque ambos usan claves, estas permanecen más ocultas en el sistema asimétrico, que trataremos a continuación.

3.8.3.2 Criptografía asimétrica

También llamada de clave pública**,** se basa en el uso de dos claves diferentes, claves que poseen una propiedad fundamental: una clave puede desencriptar lo que la otra ha encriptado, para explicarlo mejor volvamos a referirnos a Luciano Moreno que en un cuadro lo explica de la siguiente manera:



"Generalmente una de las claves de la pareja, denominada **clave privada**, es usada por el propietario para encriptar los mensajes, mientras que la otra, llamada **clave pública**, es usada para desencriptar el mensaje cifrado.

Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra, de tal forma que si dos llaves públicas son diferentes, entonces sus llaves privadas asociadas también lo son, y viceversa.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizar en sentido inverso, salvo que se conozca la clave privada, como la potencia y el logaritmo.

Ambas claves, públicas y privadas, están relacionadas matemáticamente, pero esta relación debe ser lo suficientemente compleja como para que resulte

muy difícil obtener una a partir de la otra. Este es el motivo por el que normalmente estas claves no las elige el usuario, si no que lo hace un algoritmo específico para ello, y suelen ser de gran longitud.

Mientras que la clave privada debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida ampliamente por Internet, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.

En este sistema, para enviar un documento con seguridad, el emisor (A) encripta el mismo con la clave pública del receptor (B) y lo envía por el medio inseguro. Este documento está totalmente protegido en su viaje, ya que sólo se puede desencriptar con la clave privada correspondiente, conocida solamente por B. Al llegar el mensaje cifrado a su destino, el receptor usa su clave privada para obtener el mensaje en claro.

Una variación de este sistema se produce cuando es el emisor A él que encripta un texto con su clave privada, enviando por el medio inseguro tanto el mensaje en claro como el cifrado. Así, cualquier receptor B del mismo puede comprobar que el emisor a sido A, y no otro que lo suplante, con tan sólo desencriptar el texto cifrado con la clave pública de A y comprobar que coincide con el texto sin cifrar. Como sólo A conoce su clave privada, B puede estar seguro de la autenticidad del emisor del mensaje.

Para que un algoritmo de clave pública sea considerado seguro debe cumplir los siguientes requisitos:

a) Conocido el texto cifrado no debe ser posible encontrar el texto en claro ni la clave privada.

b) Conocido el texto cifrado (criptograma) y el texto en claro debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.

c) Conocida la clave pública y el texto en claro no se puede generar un criptograma correcto encriptado con la clave privada.

d) Dado un texto encriptado con una clave privada sólo existe una pública capaz de desencriptarlo, y viceversa.

La principal ventaja de los sistemas de clave pública frente a los simétricos es que la clave pública y el algoritmo de cifrado son o pueden ser de dominio público y que no es necesario poner en peligro la clave privada en tránsito por los medios inseguros, ya que ésta está siempre oculta y en poder únicamente de su propietario. Como desventaja, los sistemas de clave pública dificultan la implementación del sistema y son mucho más lentos que los simétricos.

Generalmente, y debido a la lentitud de proceso de los sistemas de llave pública, estos se utilizan para el envío seguro de claves simétricas, mientras que éstas últimas se usan para el envío general de los datos encriptados.

El primer sistema de clave pública que apareció fue el de **Diffie-Hellman**, en 1976, y fue la base para el desarrollo de los que después aparecieron, entre los que cabe destacar el **RSA**[118] (el más utilizado en la actualidad)"

[118] El algoritmo de clave pública **RSA** fue creado en 1978 por Rivest, Shamir y Adlman, y es el sistema criptográfico asimétrico más conocido y usado. Estos señores se basaron en el artículo de Diffie-Hellman sobre sistemas de llave pública, crearon su algoritmo y fundaron la empresa RSA Data Security Inc., que es actualmente una de las más

Ahora entendamos este sistema siguen interviniendo A (emisor) y B (receptor), cada usuario tiene dos claves, una clave privada que solo él conoce, y una clave pública destinada a ser conocida por los destinatarios de los mensajes, ambas claves están entrelazadas, de manera que el mensaje cifrado con una de ellas podrá ser descifrado por la clave pareja de las mismas personas, esto cumple con el requisito de autenticidad.

Ambas claves aunque distintas se encuentran relacionas entre sí y es imposible que a partir de una clave pública se pueda conocer la privada; por un lado las claves privadas están construidas por un código alfanumérico que solo conoce el titular y por lo tanto permanece en secreto; y por otro su correspondiente clave pública esta construida por un código de letras y números, y se diferencia de la primera por que esta es del dominio público, puesto que aparece en los registros de una autoridad certificadora (tema que trataremos más adelante) como un fedatario público como un notario.

Este sistema tiene la característica de confidencialidad por que el remitente puede estar seguro que solo el destinatario, o sea el que tiene la clave privada es el que puede descifrar el mensaje sin que haya necesidad de intercambiar algún tipo de clave; esto es discutible por que la confidencialidad trae

---

prestigiosas en el entorno de la protección de datos. RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número. El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico. RSA es el más conocido y usado de los sistemas de clave pública, y también el más rápido de ellos. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Ídem.

consigo un problema ante la imposibilidad de la intervención de las comunicaciones codificadas con criptografía asimétrica; por parte de alguna autoridad ya que en cierta forma estarían ante la imposibilidad de poder descifrar información en pro de la lucha contra el delito, trayendo consigo un dilema ya que el solo nombre de las claves hace referencia a su naturaleza.

También cumple con la característica de integridad ya que ambas partes estarán seguros que los mensajes no han sido modificados en caso contrario sí el cifrado no coincide el mensaje fue alterado o sustituido en su viaje.

Quién posee una pareja de tales claves asimétricas puede firmar (firmar digitalmente) un documento informático, de modo tal que cualquiera que acceda al documento, tendrá la certeza respecto de quien envió el documento y de la integridad del mismo; para conseguir esto no tendrá más que verificar de la correspondencia entre la clave pública asociada al nombre del firmante y la clave privada con la que el documento esta firmado.

3.8.4 Propósitos por los que se cifran mensajes

Las técnicas criptográficas necesarias para brindar seguridad a los sistemas son utilizadas para los siguientes propósitos o objetivos fundamentales y a modo de resumen diremos que son:

a) “Mantener la confidencialidad del mensaje, es decir, hacer que la información transmitida a través de una red o almacenada en un sistema informático sea totalmente ilegible para quien no posea la clave para hacerla legible.

b) Garantizar la autenticidad del emisor y receptor, es decir, permitir al destinatario asegurarse de que el mensaje fue enviado realmente por quien dice ser.

c) Asegurar la integridad de la información de manera que esta no pueda ser modificada o alterada, intencional o accidentalmente. El mensaje debe llegar a su destino sin alteraciones en su contenido o en el orden de la recepción.

d) Permitir el no repudió, para poder probar fehacientemente que el usuario a enviado y recibido un mensaje, de modo que ninguna de las dos partes pueda alegar que no efectúo la transmisión.

e) Posibilitar el control de acceso, de modo que solo los usuarios autorizados y debidamente identificados puedan obtener permiso de acceso al sistema y a determinados datos.

f) Garantizar la disponibilidad es decir, asegura que la información y los sistemas se encuentren disponibles cuando sean requeridos. El objetivo es asegurar la continuidad operativa de los sistemas." [119]

Ahora bien la criptografía se convirtió en una muestra de como resolver el problema de la confidencialidad, autenticación, integridad y no repudió de la información que se trata entre el emisor y el receptor; garantizando que su intercepción sea casi imposible; por lo que entre más rápido evolucione la tecnología nuevas formas de encriptar mensajes surgirán; de todas las técnicas utilizadas hasta el momento la criptografía es una de las más usadas y confiables, en especial la criptografía de clave asimétrica o pública que fundamenta y soporta

[119] VIVIANA SARRA, Andrea, op cit, p 168.

a la denominada firma digital que conlleva al documento electrónico, que es tema de nuestro siguiente capítulo.

CAPITULO IV

FIRMA DIGITAL

4.1 Concepto

4.2 Elementos de validez

4.3 Ámbito de aplicación
- 4.3.1 Envió de documentos firmados o cifrados digitalmente
- 4.3.2 Envió de correros electrónicos con acuse de recibo
- 4.3.3 En el comercio electrónico
- 4.3.4 Sistema Electoral
- 4.3.5 Sistema de Administración Tributaria

4.4 Partes que intervienen
- 4.4.1 Usuarios
- 4.4.2 Autoridad de Certificación
- 4.4.3 Autoridad de Registro

4.5 Certificados

4.6 Seguridad informática
- 4.6.1 Public Key Infraestructure (PKI)
- 4.6.2 Función Hash

4.7 Delitos Informáticos

CAPÍTULO IV. DE LA FIRMA DIGITAL

Con el propósito de revolucionar nuestro ámbito jurídico tradicional, hoy día y en relación con el tema de esta tesis, existen nuevos conceptos que una vez que nos familiaricemos con ellos harán que no sea tan complejo su uso, ni tan lejana su implementación; como ya lo vimos en los capítulos que anteceden en años anteriores al firmar se plasmaba en papel, el que hacia a este medio el idóneo para dar forma a los actos jurídicos; pero actualmente ya existe la posibilidad de que sea sustituido por medios electrónicos, los cuales no fueron creados para menoscabar las características y ventajas que el papel confiere, si no para tratar de encontrar un equivalente para poder atribuirle el mismo reconocimiento legal; una forma de lograrlo es por medio de una firma electrónica.

4.1 Concepto

Primero que nada distingamos entre lo que es una firma electrónica y una digital, ya que ambas se usan como sinónimos y en realidad no lo son, para esto nos referiremos a los conceptos que existen sobre firma electrónica para luego analizar el concepto de firma digital.

Por firma electrónica “se entiende cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual

de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita" [120]

Así es tanto es firma electrónica la firma manuscrita digitalizada como las firmas que contienen tecnología más avanzada que se crean usando sistemas criptográficos.

El proyecto de Régimen Uniforme para la firma electrónica de UNCITRAL, en su artículo 1º dice que por firma electrónica se deben de entender los "datos en forma electrónica adjuntos a un mensaje de datos lógicamente vinculados con él y que sé utilizan para identificar al firmante del mensaje de datos o indicar que el firmante aprueba la información contenida en tal mensaje"[121]

El artículo 7 de la ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional dice que quedará satisfecho el requisito de firma en un mensaje de datos cuando:

- "Se utiliza un método para identificar a esa persona y para indicar que esa misma persona aprueba la información que figura en el mensaje de datos; y
- Cuando ese método es fiable como sea apropiado para los fines para los que se generó o comunico el mensaje de datos" [122]

Los dos artículos anteriores coinciden en mencionar las condiciones generales que se deben cumplir para que un mensaje de datos tenga la suficiente credibilidad y goce de las características de las firmas manuscritas, es decir toma en cuenta la identificación del autor y la confirmación de que el autor aprueba él contenido del mensaje; siendo estas funciones básicas de las firmas autógrafas.

---

[120] MARTÍNEZ NADAL Apol-lonia, op cit, p 41.
[121] FERNÁNDEZ DELPECH, Horacio, op cit.
[122] Ídem.

La propuesta de la Directiva del Parlamento Europeo y del Consejo, por la que se trata de establecer un marco común para la firma electrónica en su artículo 2º define a esta como ”firma en forma digital integrada en unos datos y anexa a los mismos o asociada a ellos que utiliza un signatario para expresar conformidad con su contenido y que debe cumplir con los siguientes requisitos”:

- “Estar vinculada al signatario de manera única;
- Permitir la identificación del signatario;
- Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control; y
- Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior a los mismos” [123]

Esta última definición que da el Parlamento Europeo, considera en cada uno de sus puntos las características de que gozan las firmas manuscritas al indicar que esta vinculada con el signatario se hace alusión a buscar la autenticación, confidencialidad y el no rechazo; al permitir la identificación, esto se vincula con la autenticación; al ser creada por medios que el signatario mantiene bajo su control se alude a la confidencialidad y en el último inciso se toma en cuenta a la integridad del mensaje.

Ahora bien considerando las definiciones de la firma electrónica diremos que esta puede ser equiparable a una firma manuscrita ya que ambas tienen las mismas características; por lo tanto la firma también puede ser un conjunto de datos en forma electrónica que están vinculados ya sean números o letras, que se usan para identificar al autor de un documento electrónico, para demostrar que

[123] Ídem.

una persona estuvo involucrada en la firma y que fue el autor; para así entonces asociar a la persona con el contenido del documento.

Como mencionamos al principio de este apartado la firma electrónica y la firma digital se han usado como sinónimos, situación que genera un poco de confusión al referirse a ambas.

La diferencia entre ambas radica en la encriptación, es decir en la llave pública y la privada que pueden descifrar el mensaje, imaginemos que A tiene una llave y B tiene otra con el consentimiento de A, para que pueda ver el mensaje, así de simple funciona la encriptación de la firma electrónica ya que está conformada por los datos personales del firmante y un complemento numérico que asigna una entidad administrativa haciéndola de esta forma única, por lo tanto la diferencia principal es que mientras la firma electrónica se usa en sistemas criptográficos simétricos o de clave secreta, la firma digital se usa en el sistema de criptografía asimétrica o de clave pública.

Por último diremos que el concepto de firma electrónica engloba todas las clases de métodos o símbolos basados en medios electrónicos utilizados por una persona con la intención de vincularse o autenticar un documento, a este tipo de firma se le denomina firma digital, así entonces a la firma electrónica se le debe entender como él genero, que contiene a la firma electrónica en general y a la firma electrónica segura y comúnmente llamada firma digital e incluso firma electrónica avanzada.

Entonces llamaremos a la firma electrónica simple como el conjunto de datos electrónicos que sirve solo para identificar al autor un ejemplo de estas firmas es el pasword, contrario a las firmas digitales que son las que además de

poder identificar al signatario garantiza que han crecido bajo su exclusivo control estando vinculados los datos de la firma permitiendo se detecte cualquier modificación en su contenido.

4.2 Elementos de validez

Ya que considero que una firma manuscrita se puede equipar a una firma digital, por las características que ambas poseen; para considerar a las dos como validas y para que produzcan efectos dentro del campo del derecho deben de contener los siguientes requisitos:

- Que sea una persona física quien la suscriba o una persona moral con el debido poder para hacerlo;
- Que se tenga como intención el crear, transferir, modificar o extinguir derechos y obligaciones;
- Que exista el objeto, que sea determinado o determinable, y que exista en la naturaleza;
- Que sea licito y que este dentro del comercio;
- Que halla identidad entre la persona que aparece en la declaración y al autor de la firma;
- Que no exista simulación;
- Que la persona física al momento de suscribirla se encuentre totalmente lucida sin limitación alguna de sus facultades normales;
- Que la persona tenga la capacidad para contratar y obligarse es decir que su capacidad no se encuentre limitada por alguna disposición legal;

- Que la firma no se obtenga por error, con dolo o mala fe y violencia;
- Que el emisor del mensaje tenga una clave privada y la mantenga bajo ese carácter;
- Que el receptor desencripte el mensaje con su clave pública;
- Que intervenga una autoridad certificadora

Sé que algunas de las características se refieren a los elementos de validez de los contratos, me parece que estas pueden ser de total aplicación a las firmas electrónicas, ya que son reglas de derecho que se deben practicar, y que hacen que una vez cumplidos estos requisitos se podrá establecer que nació una firma digital; por lo tanto producirá efectos y surgirán derechos y obligaciones, por que la firma en si es un acto jurídico.

A contrario una firma puede ser infectada de invalidez:

- Por no tener concordancia entre la persona que suscribe y la que aparece en la obligación;
- Que el objeto no exista o no se encuentre en el comercio;
- Que tenga un fin ilícito;
- Que exista la simulación;
- Cuando la firma se obtuvo con error dolo o mala fe;
- Que alguno de los poseedores de una clave privada la haga del conocimiento de terceros.

4.3 Ámbito de aplicación

El uso de las firmas digitales es cada día mayor en ámbitos importantes de la vida cotidiana y están por ser implantadas en otros tantos, teniendo la posibilidad de acceder a numerosos servicios que harán más sencilla la vida en sociedad. Por lo tanto algunos de los ámbitos en los que se pueden aplicar las firmas y en los que por ende traerían beneficios serian:

4.3.1 Documentación firmada o cifrada digitalmente

El envió de documentos firmados o cifrados digitalmente, como cotizaciones de bienes y servicios, resúmenes de cuenta, recibos de pago, facturas electrónicas, invitaciones, promociones, ordenes de compra, circulares, planos, tarjetas de crédito, proyectos, contratos, estos últimos pueden ser firmados simultáneamente en la red, cuando A envía a B un documento firmado digitalmente en el que asegura que este es válido, y si B puede descifrarlo entonces procede de forma análoga con el documento, ya una vez que cada parte ha leído el documento firmado y ha verificado la firma digital de la otra parte, ha quedado firmado tal contrato.

4.3.2 Correo Electrónico

El envío, firma y cifrado de correos electrónicos con acuse de recibo, los

que funcionan cuando A envía un correo a B, y solo B obtiene el correo si A obtiene un acuse de recibo de B:

a) También él envió de correos electrónicos seguros donde para hacer llegar un mensaje en forma confidencial se ha de enviar junto con el texto del mensaje, procesado mediante un algoritmo de cifrado simétrico, la clave de sesión usada se cifrara con la clave pública del receptor del mensaje para que solo este pueda descifrar la clave y con ella el resto del mensaje;

4.3.3 Comercio Electrónico

Donde es posible realizar operaciones de compra y venta, y que trae consigo seguridad al operar comercialmente, lo que depende de la disponibilidad y del amplió despliegue de sistemas de pago electrónicos que contemplan al:

a) Dinero electrónico este proporciona un sistema electrónico equivalente al dinero físico, donde intervienen un banco que suministra el servicio y proporciona el dinero electrónico donde previamente el cliente hace una solicitud de trasferencia desde su cuenta y el banco le proporciona el dinero; el cliente que va a gastar el dinero que le proporciono el banco, el cuál también mediante una transferencia paga por el producto que adquirió; el vendedor que recibe el dinero del cliente y el banco que recibe el dinero ingresado por el vendedor.[124]

En este sistema se podría pensar que existen algunos riesgos, en cuanto a la seguridad ya que no se podría saber si la persona que compra algún producto

[124] FUSTER SABATER, Amparo, et al, *Técnicas criptográficas de protección de datos*, 2ª edición, Editorial Alfaomega Ra-Ma, España, 2001, págs 190, 230 – 237.

a través de la red, lo hace en forma licita, es decir en el peor de los casos este podría ser alguien que lava dinero, por eso los sistemas que se desarrollan son casi anónimos, de tal forma que solo se podría conocer la identidad de un cliente bajo ciertas condiciones es decir por ejemplo por mandato judicial, una forma en que el vendedor puede examinar la autenticidad y la integridad de la compra es con la correspondiente clave pública del banco suministrador.

b) Cheques electrónicos, en este sistema de pagos deben concurrir el cliente y el banco, y el vendedor y su banco y una cámara de compensación que procese los cheques entre los diferentes bancos, funciona cuando el cliente realiza una compra y envía el cheque electrónico al vendedor y este lo valida con el banco, así se completa la transacción, el vendedor envía el cheque a su banco para depositarlo y el banco del vendedor envía el cheque a la cámara de compensación para cobrarlo, la cámara acude al banco del cliente para transferir el dinero al banco del vendedor, que actualiza su cuenta. El banco del cliente también debe actualizar su cuenta.[125]

La forma de corroborar la autenticidad es por medio de la clave privada del cliente y que el vendedor verifica con su clave pública, este sistema de pago trae consigo ventajas en cuanto al tiempo de elaboración se refiere.

c) Pagos con tarjeta de crédito, para esta forma de pagos existen varios protocolos[126] de seguridad para realizar pagos con tarjeta de crédito uno de ellos

---

[125] Ídem.

[126] Protocolo "se entiende que nos referimos al Protocolo de Control de Transmisión / Protocolo de la Internet (TCP/IP) que es un lenguaje que las computadoras en la Internet usan para comunicarse entre ellas. El TCP/IP divide la información que envía en packets y transfiere los packets por la Internet, cuando uno envía información por la Internet, esta se descompone en piezas más pequeñas llamadas packets, cada packet viaja

es el llamado SET desarrollado por Visa y Master Card, los elementos que integran a este protocolo son: un centro emisor de tarjetas de usuario o sea la institución financiera que emite las tarjetas, el usuario de la tarjeta es decir el dueño de la tarjeta bancaria autorizado por un centro emisor; el comerciante que acepta los pagos electrónicos; la entidad financiera que da soporte a los comerciantes; la pasarela de pago que es el sistema que proporciona servicios de comercio on-line a los vendedores; las autoridades de certificación que autentican las claves públicas de los elementos integrantes del sistema.

Este sistema de pagos funciona cuando un usuario decide realizar una compra, para lo que envía una instrucción de pago on-line al vendedor, el comerciante también se comunica on-line con su entidad financiera a través de la pasarela de pago, para que autorice y capture la transacción, así la entidad financiera del comerciante captura la información y puede solicitar una transacción al centro que emite la tarjeta y por último mediante una cadena de confirmación del centro emisor a la entidad financiera de esta al comerciante y del comerciante al cliente, permite al dueño de la tarjeta realizar la compra.[127]

Este sistema SET usa la criptografía asimétrica y por lo tanto puede cifrar instrucciones de pago para asegurar el número de la tarjeta, autentifica a las tres partes que intervienen en este sistema de pagos primero a los propietarios de las tarjetas ante los comerciantes y las entidades financieras para proteger contra el robo de tarjetas; segundo al comerciante ante el cliente y la entidad financiera

---

independientemente y puede tomar una ruta diferente para llegar al destino deseado, cuando sucede lo anterior el TCP/IP se asegura que todos los packets han llegado satisfactoriamente". APRENDA COMPUTADORAS E INTERNET VISUALMENTE, Editorial Reader's Digest S.A. de C.V., México 1999, p 206.

[127] Ídem.

como protección contra suplantadores; y tercero a las entidades financieras ante los propietarios de tarjetas y ante los comerciantes para evitar que un suplantador consiga datos sensibles contenidos en las instrucciones de pago.

4.3.4 Sistema Electoral

Uno de los ámbitos en donde se están comenzando a usar las firmas digítales, es en el sistema electoral mexicano en donde la pregunta de hoy es ¿Cómo pueden varias personas emitir su voto por medio de la red, de modo que tales votos sean contabilizados en el resultado de la votación pero de manera que sus votos permanezcan en secreto?, la respuesta a esta pregunta lo encontramos en la implantación de una mesa electoral que comprobara la legitimación de cada uno de los votantes, para eso cada votante enviara su voto y contara con un número secreto de identificación, el resultado de la votación es publicado en una lista que contiene el conjunto de identificaciones secretas que han optado por tal opción, ahora de esta manera se podría saber lo que han votado cada votante, por eso se implementan dos agencias una para legitimar los votos y otra que calcula y hace público el resultado. [128]

Actualmente en México se encuentra en estudio el primer prototipo de votación electrónica, el objetivo de este es utilizarlo para llevar a cabo un proyecto de votación electrónica en el ámbito nacional, el que tomaría elementos del modelo tradicional de votación y los combinaría con innovaciones tecnológicas y tendría por objeto la automatización del proceso de recepción del voto de esta

[128] Ídem.

forma se simplificarían las tareas de la jornada electoral. A nuestro parecer el voto electrónico funcionaria de la siguiente manera:

- El ciudadano vota por el partido de su preferencia, en una casilla sin tener algún vinculo con el comunicador o con otras casillas, lo que garantiza que la votación sea única en cada casilla;
- La manera de acceder al sistema para emitir el voto es por medio de una tarjeta especial que contiene un código de acceso que se genera codificado con un esquema de seguridad que no permite descifrar la información contenida en ella;
- El voto se emite mediante el tacto de una pantalla electrónica, que permite al votante una vez que verificado el código de acceso correspondiente accede a la boleta virtual para que emita el voto;
- El software proporciona a los votantes la información necesaria de los candidatos;
- Una vez que el ciudadano vota el sistema emite un comprobante impreso y guarda la información.[129]

Algunas de las ventajas de este sistema son que se eliminaría el uso físico de boletas y actas electorales; suprime el recuento de las boletas; agiliza la entrega de los resultados; reduce costos financieros; agiliza la emisión del sufragio y da cierta transparencia y certidumbre en cada voto expresado.

---

[129] MARTÍNEZ CASTAÑO, Juan Antonio, Voto Electrónico y Software Libre, 2000 [En Línea]Disponible:http://oasis.dit.upm.es/~jantonio/documentos/voto-electronico/article.html, 14 abril de 2006.

4.3.5 Sistema de Administración Tributaria

En el SAT ya se usa la firma digital introduciendo reformas a la legislación fiscal federal con el objeto de permitir que los contribuyentes puedan realizar tramites ante el Estado como presentar sus declaraciones fiscales o efectuar el pago de impuestos en forma electrónica.

Las personas que de cuerdo a las disposiciones fiscales tengan la obligación de presentar solicitudes en materia de registro federal de contribuyentes, ya sean declaraciones o avisos ante las autoridades fiscales así como expedir constancias o documentos lo harán de acuerdo a las formas que aprueba la Secretaria de Hacienda y Crédito Público.

Desde el año de 1998 algunas personas morales (grandes contribuyentes) pueden presentar sus declaraciones anuales al SAT por medios electrónicos firmando electrónicamente con un certificado digital que el propio SAT les proporciona.

Lo anterior seria discutible ya que en ese supuesto el SAT tendría una doble función es decir seria juez y parte ya que por un lado emitiría el certificado y por el otro será ante la autoridad ante la que se presentaría.

A partir del año 2002 se determino de conformidad con él artículo 31 del Código Fiscal de la Federación que “los contribuyentes obligados a la presentación de pagos provisionales mensuales debían presentar a través de medios electrónicos las declaraciones o avisos correspondientes. En dicha disposición se autoriza a los contribuyentes a presentar de manera física la

declaración o aviso en cuestión para poder tener el sello de recibido de la autoridad fiscal competente para tales efectos”

A través de dicha disposición se permite a los contribuyentes a realizar diversos tramites ante el SAT mediante el uso de medios electrónicos, sin perjuicio de que se presenten ante la propia autoridad los documentos que fueron objeto del tramite por medios electrónicos con el fin de acreditar que estos fueron presentados.

Este sistema funciona de la siguiente manera:

- El contribuyente obtiene una identificación electrónica que este obtiene a través de la pagina de Internet del SAT, en la generación de esta clave el SAR asume las funciones de entidad certificadora (tema que será analizado mas adelante).

- El contribuyente presenta sus declaraciones ya sean complementarias, pagos mensuales provisionales o definitivos, etc., y en general cualquier tramite por el que tenga que cumplir con una obligación fiscal.

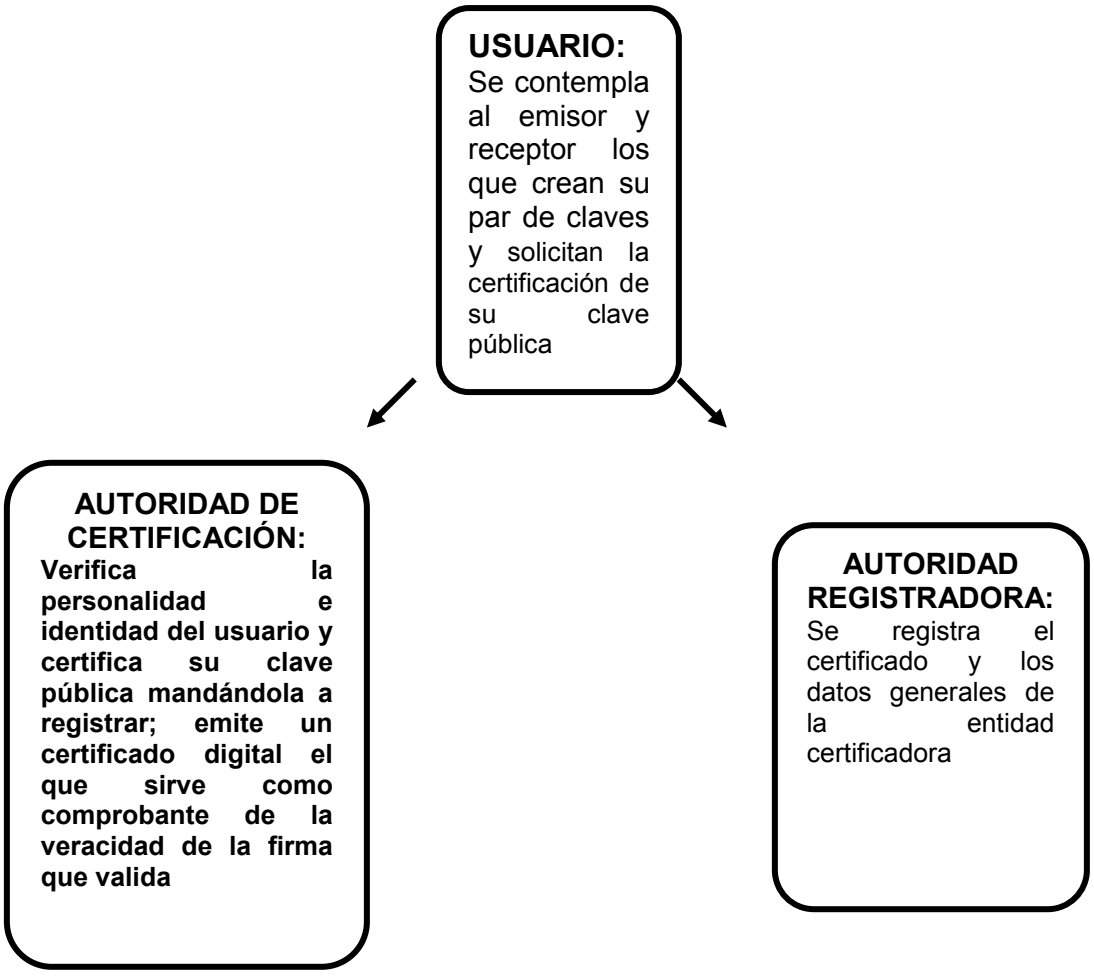
- Si el particular realiza el pago este se hace por transferencia de fondos, una vez hecho esto las instituciones bancarias que están autorizadas para operar de esta manera envían al contribuyente por la misma vía electrónica el acuse de recibo que contendrá el sello digital generado por las propias instituciones con el fin de autenticar la operación realizada y en su caso el pago.

Hay que tomar en cuenta que la forma en que los contribuyentes pueden establecer su identidad es a través de los medios de identificación automatizados que las instituciones de crédito tengan establecido con sus clientes los medios de identificación electrónica confidencial que se generen por los contribuyentes

mediante los desarrollos tecnológicos del SAT, así como el uso de la tarjeta tributaria, sustituyen a la firma autógrafa y por lo tanto producen los mismos efectos que las leyes otorgan a los documentos correspondientes teniendo el mismo valor probatorio.

4.4 Partes que intervienen

En la generación de una firma digital intervienen personas e instituciones sin las cuales este tipo de firma no tendría vida jurídica propia, para crear un mejor entendimiento de las partes que intervienen en la generación de una firma electrónica y cual es la función de cada uno de ellos ejemplificaremos en el siguiente cuadro:



4.4.1 Usuarios

Hoy en día crece el número de usuarios de algún medio electrónico por el cual puedan contratar u obligarse:

a) Emisor:

Este es el autor del documento, y el que cuenta con un par de claves una pública y una privada que le son asignadas por una autoridad de certificación, la primera de las claves como su nombre lo indica es pública y por lo tanto conocida por cualquier persona que pretenda establecer una relación a través de medios electrónicos, y la segunda de las claves es privada y por lo miso solo conocida, resguardada y mantenida en secreto por el emisor del mensaje esta le sirve para cifrar la información y enviarla a la persona con quien va a contratar y obligarse.

A este usuario se le define en el Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en materia de firma electrónica, de junio de 2003, el que ya fue analizado en él capítulo segundo de este trabajo, y define al emisor como: “Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario”.[130]

[130] DIARIO OFICIAL DE LA FEDERACIÓN de 16 de junio de 2003.

b) Receptor:

Es la persona a quien va dirigida la información, y que cuenta con un software que previa introducción en el mismo de la clave pública del remitente descifrará el mensaje que fue cifrado por el autor, y luego calculara el extracto hash que le correspondería al texto del mensaje y si el texto coincide la operación es valida; este también cuenta con su par de claves.

En el mismo Decreto al que ya aludimos también define al receptor o destinatario como: “La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje”.[131]

Para ambos usuarios es obligación el adoptar las medidas de seguridad necesarias para mantener bajo su control la información que se transmita, respetando el estricto significado de su par de claves.

4.4.2 Autoridad de Certificación (AC)

Figura importante en la infraestructura con la que se debe contar par lograr una firma digital, tiene sus orígenes en Estados Unidos de Norte América por la necesidad de autenticar principalmente actos de comercio; en donde se comenzaba a usar la firma digital la que sabemos que requiere de la existencia de un certificado al cual se le ha aplicado una llave privada y que es preciso desencriptar con el uso de la llave pública para que después mediante la función

[131] Ídem.

hash se compruebe y conozca el mensaje enviado, todo esto conlleva a una tercera parte intervenga con el fin de autenticar la información.

De acuerdo a la anterior, la autoridad certificadora, también es llamada por algunos autores como tercera parte de confianza, las que además de facilitar la distribución de una clave pública, permiten vincular la identidad de una persona a una clave pública determinada a través de la emisión de certificados. Esas terceras partes de confianza cuentan con ciertas medidas de seguridad denominados protocolos.[132]

Así entonces las terceras partes de confianza son entidades en las que confían las partes que intervienen en una transacción para proporcionar servicios de seguridad, apoyándose para ello en un certificado y cuya función principal es unir un par de claves con la firma de un determinado suscriptor, el certificado es firmado por dicha autoridad cuya clave pública podrá ser a su vez consultada por el receptor y así sucesivamente, hasta que obtenga la confianza que necesita. Una vez creada la firma digital por la entidad de certificación previa identificación

[132] Los protocolos, especifican las reglas del comportamiento que se deben seguir para desarrollar mecanismos de seguridad fiables, estos protocolos en terminología inglesa son los Trusted Tirad Party TTP y son los siguientes: **a)** protocolos auto verificables: en estos cada una de las partes se da cuenta si la otra parte actúa deshonestamente durante el transcurso de la operación; la firma digital es un elemento básico de este tipo de protocolos ya que no necesita de la intervención de una autoridad de certificación para determinar si es valida su firma; **b)** protocolos arbitrados: en estos la autoridad de certificación participa en las transacciones para asegurar que ambos partes que intervienen actúan según lo pactado por el protocolo; y **c)** protocolos notariales: la autoridad de certificación además de que garantiza la correcta operación, permite juzgar si ambas partes actuaran por derecho según la evidencia de los documentos aportados por los participantes e incluidos en el protocolo notarial. En estos casos se añade la firma digital del notario a la transacción pudiendo este testificar luego en caso de alguna disputa. PÉREZ FONTAINE, Rodolfo, *La tecnología digital*, Editorial Dykinson, México, 2000, págs 78-79

de la persona su certificado deberá ser agregado a la base de datos existente para hacer posible su consulta en un futuro.[133]

Ahora bien una autoridad de certificación debe reunir los requisitos que determine la ley como:

- Los cocimientos técnicos y experiencia necesaria de manera que ofrezca confianza, fiabilidad y seguridad;
- Recursos y capacidad financiera para asumir la responsabilidad por el riesgo de perdida;
- Aprobación del equipo y programas;
- Mantener un registro de auditoria y realización de auditorias por una entidad independiente;
- Disposiciones para proteger su propia clave privada;
- Capacidad para intercambio datos con otras autoridades certificadoras;
- Procedimientos de revocación en caso de que la clave criptográfica se haya perdido o hay quedado expuesta.[134]

Por otro lado dentro de sus funciones se encuentran las de:

- Generación y registro de claves;
- Certificación y registro de una operación se ha llevado a cabo por vía electrónica, otorgándole certeza de que el receptor del mensaje sepa que el emisor del mismo sea realmente quien dice ser;

---

[133] MARTINEZ NADAL, Apol-lonia, op cit, págs 67-68.
[134] Anguiano & Asociados, Abogados, Departamento de Comercio Electrónico, Requisitos de las Autoridades de Certificación según el Grupo de Trabajo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, [En Línea]. Disponible: http://www.arrakis.es/~anguiano/artautcert.html, 15 abril de 2006.

- Identificación de peticionarios de certificados;
- Emite certificados al garantizar su identidad por medio de una firma digital;
- Almacena en la AC de su calve privada;
- Mantiene guías al día para conocer las claves públicas de aquellas o aquel con quien desea tener contacto vía red; y
- Mantiene listas de claves vigentes y revocadas en un especie de directorio.[135]

Para resumir la autoridad certificadora tiene la labor de establecer una liga entre el firmante y las llaves usadas para crear la firma digital; en esencia esta autoridad revisa los documentos de identificación del firmante como licencia, pasaporte o cualquier documento que ratifique su persona, posteriormente certifica que la persona que esta utilizando la llave sea realmente la persona que dice ser, por lo tanto cualquiera que quiera verificar una firma digital debe confiar en la autoridad de certificación en lugar de personalmente revisar los documentos de identificación del signatario.

4.4.3 Autoridad de Registro (AR)

Esta es la encargada de la autenticación de la identidad de los usuarios de la autoridad certificadora; es el intermediario entre los usuarios y la autoridad certificadora; la calidad del proceso de autenticación de esta autoridad es el que determina el nivel de confianza que se tendrá a los certificados emitidos por estas.

---

[135] Ídem.

En nuestro país en el ámbito financiero el Banco de México es el que cuenta con las atribuciones para implementar y regular el uso de los medios electrónicos y sistemas de seguridad en los sistemas de pagos, en la transferencia de datos y en la celebración de operaciones activas, pasivas y de servicios de intermediación financiera.

Es por lo anterior que el Banco de México esta promoviendo una infraestructura extendida de seguridad por medio de una agencia registradora central que se encarga de supervisar las claves públicas, así como autorizar la operación de las demás entidades que forman parte del esquema, de ella dependen directamente tanto la autoridad de registro como la de certificación contemplando que ambas funciones las puede desarrollar una sola empresa.

Entonces la agencia registradora central tiene la responsabilidad del registro, publicación y en su caso revocación de certificados, y bajo lo anterior en nuestro país el Banco de México participara en principio como agencia registradora central en las operaciones que se celebren con las instituciones de crédito.[136]

Por último será el receptor del mensaje quien decidirá si otorga la suficiente confianza a la AR que emitió el certificado con el que se ha firmado el mensaje, estas AR son las que solucionan el único punto débil que tienen los sistemas basados en criptografía de clave pública. Estas también son llamadas terceras partes confiables por eliminar el riesgo que existe para el usuario decidir

[136] VILLALPANDO MORALES, Carlos, *Transacciones electrónicas*, Editorial Destino, Argentina, 1999, p 223-225

si confiaba o no en la identidad del que firmaba ya que se encarga de identificar con total garantía al autor del mensaje.

4.5. Certificados

Para que una clave pública se pueda considerar como valida y que esta asociada a un usuario determinado debe tener un certificado que así lo demuestre. Desde el punto de vista técnico un certificado es "un registro electrónico que atestigua que una clave pública pertenece a determinado individuo o entidad".[137]

Podemos preguntarnos ¿cómo es que sabemos que A y B tienen asignados las llaves públicas que dicen tener?, ¿Cómo tengo la certeza de que la clave pública de un usuario corresponde a el y no ha sido falsificada por otro? y ¿quien verifica la identidad del poseedor de la clave pública?, todas estas preguntas encuentran su respuesta en la figura de los certificados digitales, los que contienen el nombre de la persona y su llave pública y esta firmado con la llave privada de una autoridad certificadora o los ciber fedatarios., adicionalmente también contienen:

- El código identificativo único del certificado;
- La identificación del prestador de servicios de certificación que expide el certificado;

[137] RAMOS SUÁREZ, Fernando, Como aplicar la nueva normativa sobre firma electrónica, Noticias jurídicas del 25 de febrero de 2000, [En línea]. Disponible: http://www.noticiasjurídicas.com/, 15 abril de 2006.

- La firma electrónica del prestador de servicios de certificación que expidió el certificado y que da fe de que el certificado expedido es valido y se emitió de acuerdo a las practicas de certificación;

- La identificación del signatario por su nombre apellido etc, en fin toda la información que pueda ser relevante para el uso del que será objeto el certificado;

- Los datos de verificación de la firma, la clave pública que correspondan los datos de firma que se encuentren bajo el control del signatario, es decir la clave privada, de manera que se produce una vinculación exclusiva del interesado con las claves; la clave pública es la que permite a su vez verificar la autenticidad de la firma electrónica;

- El conocimiento y el fin del periodo de validez del certificado fuera de los cuales no podrá usarse;

- Los limites del uso del certificado si se prevén por ejemplo en la compra por medio de la red acceso a bancos etc; y

- Los limites del valor de las transacciones por las que pueda usar el certificado si se establecen, así se controla que con un certificado no puedan efectuarse compras por un importe mayor a un valor especificado en el mismo.[138]

Ahora bien un certificado nos es útil para:

- Comprobar que la clave pública de un usuario, cuyo conocimiento es imprescindible para autenticar su firma electrónica;

- Por lo tanto atestigüen la validez de la identidad de un individuo o entidad;

---

[138] CIENFUEGOS SUÁREZ, Juan, *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Editorial España, España, 1998, págs 98 a 100.

- Permitirán a sus titulares realizar una gran cantidad de acciones a través de Internet, es decir acceder por medio del navegador a sitios web restringidos a los cuales les deberá presentar previamente el certificado cuyos datos serán verificados;

- Otra razón por la que es útil es por que permiten la verificación de la premisa que una llave pertenecer de hecho a un individuo el principal inconveniente del uso de claves pública es el modo de asociación de los pares llave pública y llave privada con personas físicas. La solución la aportan las autoridades de certificación (notarios electrónicos) que son entes fiables y ampliamente reconocidos que firman las claves públicas de las personas rubricando con su firma su identidad.[139]

Ahora bien el funcionamiento de un certificado es de la siguiente manera:

El certificado digital incorpora información sobre el usuario información que debe ser trasladada por algún tipo de autoridad competente que dota así de validez al documento acreditativo.

Aquí es donde entra la función de la autoridad de certificación AC o prestador de servicios de certificación, la que se encarga de verificar la identidad de los solicitantes de certificados además de crear y emitir a los solicitantes dichos certificados y publicar las listas de revocación de los mismos.

Tipos de certificados:

- De identidad que son los más usados actualmente por los criptosistemas de clave pública y ligan una identidad personal (usuario) o digital (equipo software) a una clave pública;

---

[139] Ídem.

- De autorización o potestad que son los que certifican otro tipo de a tributos del usuario distintos a la identidad;

- De transacciones aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero; y

- De tiempo o estampillado digital de tiempo permiten dar fe de que un documento existía en un instante determinado de tiempo.[140]

Ventajas de un certificado digital:

- Por su estructura matemática especial pueden ser verificados con una veracidad del 100% es decir seria muy difícil duplicar un certificado digital;

- Aceptación internacional por los estándares establecidos;

- Provee autenticación para tener transacciones seguras;

- Permite las mismas garantías de la firma física;

- Cumple con el requerimiento de auditorias internas;

- Permite seguridad en transacciones electrónicas;

- Los costos operativos de generación y administración de certificados son bajos a largo plazo.

- Los certificados implementados dentro de un esquema PKI (public key infraestructure, sistema que será analizado más adelante) logran que la seguridad como un todo sea más sencilla de monitorear.

Algunas recomendaciones para el uso de certificados:

- Compromiso de la clave privada del usuario, en caso de que una clave privada cayera en manos de alguien desconocido o de que el usuario olvidare la

[140] Cámara Nacional de Comercio, Servicios y Turismo de Chile, Entidad de Certificación electrónica, Prácticas de Certificación Digital (PCD) CNC-ONCE [En línea]. Disponible: http://www.cnc-once.cl/prac_cert.htm, 15 abril de 2006.

contraseña que protege a su clave privada, se debe dar aviso a la autoridad certificadora para que el certificado sea revocado;

- Compromiso de la clave privada de la autoridad certificadora, en el supuesto de que la clave privada de una AC llegare a caer en manos de un desconocido, esta deberá cambiar su calve quedando así invalidados todos los certificaos reconocidos y emitidos hasta ese momento; es por eso que las políticas de seguridad de una AC deben ser lo suficientemente duras como para que lo anterior no llegare a suceder;

- Cambio de los datos del certificado en caso de que el usuario cambiare de trabajo, de lugar de residencia, etc, motivos que pueden justificarla emisión de un nuevo certificado que refleje verazmente la nueva información personal del titular y la invalidación del certificado antiguo;

- Violación de la política de la autoridad certificadora; si un usuario violo las normas de certificación de la autoridad certificadora esta puede decidir revocar su certificado;

- Expiración del certificado, los certificados tienen un tiempo de vida limitado, al final de este tiempo dejan de ser validos, para lo cual el usuario debe solicitar su renovación a la AC que se lo emitió.

4.6 Seguridad informática

Hoy en día es cada vez mayor el uso de tecnologías para comunicarse, por lo tanto es necesario que existan sistemas de seguridad que ofrezcan las mismas funcionalidades de los documentos físicos.

4.6.1 Public Key Infraestructure (PKI)

Es un termino usado para referirse a la infraestructura de seguridad, la que se basa en criptografía de clave pública la que permite la gestión de certificados digitales y cuyos orígenes se remontan a un artículo seminal de Diffie y Hellman de 1976 donde explicaban la idea revolucionaria de servirse para la operaciones criptográficas de una pareja de claves, una pública conocida por todos y una privada solo conocida por el usuario a quien le fue asignada.

La PKI proporciona cuatro funciones principales de seguridad para las transacciones comerciales**:**

- Confidencialidad;
- Integridad;
- Autenticación;
- No repudio.

Aplicaciones para PKI:

- Transacciones financieras en Internet;
- Correo Electrónico;
- Comunicación entre servidores web.

Características de los certificados PKI:

- Basados en estándares internacionales;
- Compatibles con diversas aplicaciones y productos;
- Tienen una interoperabilidad segura en todo el sistema;
- Un uso de una firma digital y aplicaciones de intercambio de llaves;

- Cumplen con la legislación y regulaciones nacionales e internacionales.[141]

Una infraestructura de clave pública es una combinación de productos de hardware y software, políticas y procedimientos, ofrece la seguridad básica requerida para llevar acabo negocios electrónicos de forma que los usuarios, que no se conocen entre si o están muy alejados entre si, pueden comunicarse con seguridad a través de una cadena de confianza. La PKI se basa en entidades digitales conocidas como certificados digitales que actúan como pasaportes electrónicos y vinculan la firma digital del usuario a su clave pública.[142]

Una PKI incluye:

- Una política de seguridad (certificados digitales)
- Autoridad de certificación
- Autoridad de registro
- Sistema de distribución de certificados
- Aplicaciones habilitadas por PKI

Es decir incluye una o varias autoridades de registro para certificar la identidad de los usuarios; una o varias autoridades de certificación que emitan los certificados de clave pública; un lugar para almacenar certificados; listas de revocación de certificados con certificados suspendidos o revocados.

Por ultimo algunos sistemas de PKI se gestionan mediante autorizadores de certificados comerciales (CCA) o terceras partes seguras, y, por lo tanto requieren un CPS este es un documento en el que se detallan los procedimientos

---

[141] LUCENA, Manuel, Kriptopolis, privacidad, identidad, seguridad, Mensajería Instantánea y segura, 27 mayo 2003 [En línea]. Disponible: http://www.kriptopolis.org/node/1185, 15 abril de 2006.

[142] CIENFUEGOS SUÁREZ, Juan, op cit, p 98.

operativos sobre como ejecutar la política de seguridad y como aplicarla a la practica. Por lo general incluye definiciones sobre como se construyen y operan los CA como se emiten, aceptan y revocan los cerificados y como se generan y registran y certifican las claves, donde se almacenan y como se ponen a disposición de los usuarios. Las autoridades certificadoras tienen un conjunto de políticas operativas que describen la implantación y apoyo a la políticas de seguridad condensadas a un detallado documento conocido como Declaración de Practicas de Certificación (CPS) estas políticas incluyen procedimientos de verificación de identidad rango de usuarios a certificar y el ciclo de vida de los certificados. [143]

4.6.2 Función “hash”

Una forma de darle seguridad a la firma digital, es a través de las denominadas funciones “hash”: ”El “hash” es entendido como el algoritmo que trasforma una secuencia de bits en otra menor, y que se aplica tanto para la creación como para la verificación de la firma digital. Dado que la aplicación de criptografía asimétrica sobre la totalidad del mensaje puede resultar costosa, se suele aplicar sobre el mensaje inicial una función “hash”, obteniéndose un resumen denominado compendio del mensaje o huella digital que se caracteriza por ser irreversible es decir a partir del resumen no puede obtenerse el mensaje completo inicial, y por ser único es imposible obtener un mensaje que produzca el

[143] FERNÁNDEZ MACIA, Enrique, *La protección internacional de los programas de ordenador*, Editorial Comares, España, 1998, págs 113, 119.

mismo resumen “hash”, de tal manera que se asegura la integridad del mismo, ya que cualquier cambio en el mensaje produciría un resumen o “hash” diferente. El “hash” es cifrado con la clave privada de criptografía asimétrica del firmante, remitiéndose el mensaje original y su resumen o “hash” conjuntamente. Así entonces, el receptor cuenta con dos elementos con los que se puede verificar la firma”

Estas funciones son usadas para comprobar la integridad de los datos de algún documento enviado a través de medios electrónicos, ya que esta función reduce el mensaje original a un valor resumen de menor tamaño, de manera que este sirve como representación compacta del anterior.

La verificación de la firma digital es el proceso de comprobación por referencia al mensaje original y una clave pública dada, determinado de esta forma si la firma digital fue creada para este mismo mensaje utilizando la clave privada que corresponde a la clave pública referida. para ello el verificador realizara dos operaciones descifrara el “hash” firmado con la clave pública del emisor aplicando la clave pública del mismo; y aplicara la función de “hash” sobre el mensaje completo que ha obtenido. Si el “hash” recibido y descifrado y el segundo “hash” obtenido coinciden, el destinatario tiene la seguridad de que el mensaje recibido ha sido firmado por el emisor con ese contenido, al contrario si uno u otro de los dos elementos ha sido alterado en algún momento, no habrá coincidencia en los dos resúmenes”. [144]

[144] LLANEZA GONZÁLEZ Paloma, op cit, págs 51 - 52.

En estas funciones se da cumplimiento a las características de las firmas como la integridad cuando el mensaje no fue alterado, el no rechazo cundo el autor no niega ser el autor.

Por último esta función es usada en la criptografía asimétrica, donde el certificado o resumen del texto quedara representado numéricamente, y el que origino el mensaje es quien con su llave privada encripta el mensaje y el destinatario con su clave pública lo desencripta teniendo este último la seguridad de que el primero es el autor del documento, y que además el documento no sufrió modificación, este cerificado con función “hash” aplicada y luego codificado de manera inversa al documento constituye la firma digital.

4.7 Delitos informáticos

Los delitos informáticos son aquellos que están íntimamente ligados a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información (datos programas, documentos electrónicos, dinero electrónico, información etc) entre los delitos podemos mencionar:

- Acceso no autorizado
- Destrucción de datos;
- Infracción de los derechos de autor;
- Infracción del copyright de bases de datos;
- Interceptación de un e mail.

En nuestro país ya se esta trabajado en proyectos legislativos relativos al comercio electrónico, y aunque el tema central de este trabajo no es el comercio electrónico si haremos referencia a esta ley ya que el procedimiento en que se lleva a cabo una firma digital es a través de medios electrónicos.

La ley en la que se esta trabajando en México, pretende adecuar la legislación penal mexicana a normas internacionales, procurando combatir la piratería, hanckers y crackers, así como la prohibición de transmitir material pornográfico a través del Internet. [145]

Julio Téllez clasifica a los delitos informáticos basándose en 2 criterios:

- Como instrumento o medio se tienen a las conductas criminó genas que se valen de computadoras como método, medio o símbolo en la emisión del ilícito y;

- Como medio y objetivo en esta categoría se enmarcan las conductas criminó genas que van dirigidos en contra de la computadora, accesorios o programas como entidad física.[146]

Maria de la Luz Lima los clasifica en tres categorías:

- Los que utilizan la tecnología electrónica como métodos: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado licito.

---

[145] NAVA GARCÉS, Alberto Enrique, *Análisis de los delitos informáticos*, Primera Edición, Editorial Porrua, México 2005, p 205.
[146] TÉLLEZ VALDEZ, Julio, *Derecho Informático,* Segunda Edición, Editorial Mc Graw Hill, México 1996, págs 103 y 104.

- Los que utilizan la tecnología electrónica como medio son conductas criminó genas en donde para realizar un delito utilizan una computadora como método o símbolo; y

- Los que utilizan la tecnología electrónica como fin conductas criminó genas dirigidas contra la entidad física del objeto o maquina electrónica o su material con objeto de dañarla.[147]

Ahora bien hay delitos informáticos los cuales son reconocidos por Naciones Unidas:

- Manipulación de programas que consiste en que el delincuente tiene conocimientos técnicos concretos de informática, así el delito conste en modificar programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas;

- Manipulación d datos de entrada también conocido como sustracción de datos representa el delito informático más común ya que es fácil de hacer y difícil de descubrir;

- Manipulación de datos de salida que se realiza fijando un objetivo al funcionamiento del sistema informático; el ejemplo más común es el fraude que se hace a los cajeros automáticos por medio de la falsificación de instrucciones para la computadora n la fase de adquisición de datos;

Igualmente considera a las falsificaciones informáticas:

- Como objeto cuando se alteran datos de los documentos almacenados en forma computarizada;

---

[147] LIMA DE LA LUZ, Maria, *Delitos electrónicos en criminalía*, Academia Mexicana de ciencias penales, Editorial Porrua, México, No 1-6 Año L. Enero –Junio 1984, p 100.

- Como instrumentos las computadoras pueden usarse también para efectuar falsificaciones de documentos de uso comercial como fotocopiadoras de alta resolución, que crean documentos falsos sin tener que recurrir al original.

También considera a los daños o modificaciones de programas o datos computarizados:

- Sabotaje acto de borrar, suprimir o modificar sin autorización funciones o datos de la computadora para que el sistema no pueda funcionar normalmente;

- Virus que son claves programadas que se adhieren a los programas legítimos y se propagan a otros programas informáticos.[148]

Por ultimo existen los piratas informáticos o hanckers en donde este delincuente aprovecha la falta de rigor de las medidas de seguridad, los piratas se hacen pasar como usuarios legítimos del sistema accediendo a el desde un lugar exterior situado en la red de telecomunicaciones.

[148] FERNÁNDEZ DELPECH, Horacio, op cit.

CAPITULO V

EL EJERCICIO DE LA FE PUBLICA DEL NOTARIO

5.1 Procedimiento

5.2 La firma en la legislación notarial

5.3 Proyecto de un Cybernotario

5.4 Escritura Publica

5.5 Protocolo Electrónico

5.6 Instituciones que auxilian al Notario en su labor
- 5.6.1 Archivo general de notarias
- 5.6.2 Registro Público de Comercio y de Patrimonio del Inmueble Federal

5.7 Conservación de datos (Norma Oficial Mexicana)

5.8 Efectos y alcance legal de la firma electrónica

5.9 Propuesta, iniciativas y necesidad de legislar

CAPÍTULO V. EL EJERCICIO DE LA FE PÚBLICA DEL NOTARIO

Recordando lo que ya estudiamos en los capítulos que anteceden, y tomando en cuenta los conceptos ya analizados, los cuales en su conjunto nos llevaran a establecer el rol que juega un notario público en la firma y certificación digital y que por lo tanto determinaran el momento en que este funcionario público da fe y certifica que se ha llevado a cabo un acto jurídico por medio de una firma digital, analicemos la función especifica de este fedatario.

5.1 Procedimiento

El procedimiento de firma y certificación digital se da de la siguiente manera y es aquí donde cada uno de los usuarios tienen su ocupación definida:

Emisor:

1. - Genera un mensaje claro.
2. - Genera un resumen del mensaje con la función hash apropiada.
3. - Cifra el resumen del mensaje con el algoritmo de clave asimétrica, utilizando la clave privada del emisor.
4. - Codifica el resumen cifrado en la forma adecuada y lo añade al mensaje saliente.
5. - Envía el resultado de los pasos anteriores vía Internet.

Receptor:

1. - Recibe el mensaje y extrae el resumen cifrado que se ha añadido.
2. - Obtiene la clave pública del emisor.

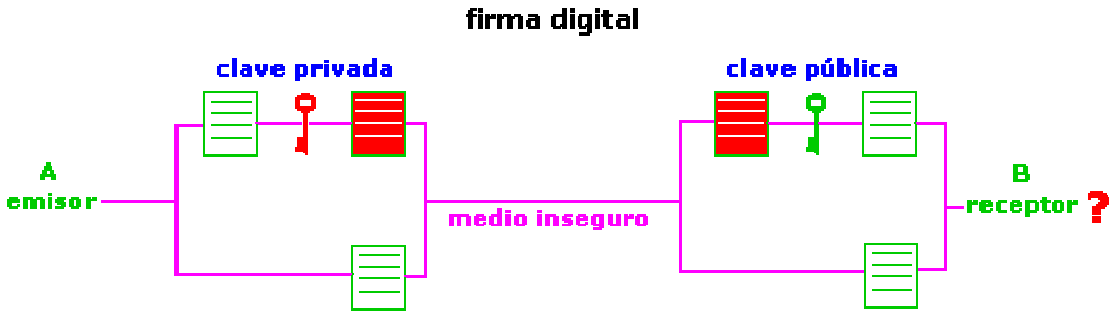
3. - Descifra el resumen utilizando la clave pública del emisor.

4. - Calcula el resumen a partir del mensaje en claro recibido.

5. -Compara el resumen calculado a partir del mensaje y el resumen descifrado

Si ambos resúmenes coinciden, se puede tener la seguridad sobre la identidad del emisor y la integridad del mensaje.

Para comprender mejor lo anterior nos remitiremos de nuevo al texto de Luciano Moreno que hace en un esquema muestra a la firma digital básica, y que también alude al tipo de procedimiento que se lleva a cabo para su generación:



Luciano Moreno considera que el proceso de firma digital consta de dos partes bien diferenciadas:

"1. **Proceso de Firma**: en el que el emisor encripta el documento con su llave privada, enviando al destinatario tanto el documento en claro como el encriptado.

2. **Proceso de Verificación de la Firma**: el receptor desencripta el documento cifrado con la clave pública de A y comprueba que coincide con el documento original, lo que atestigua de forma total que el emisor del mismo ha sido efectivamente A.

El método de la firma digital no sólo proporciona autenticidad al mensaje enviado por A, si no que también asegura el no repudio, ya que sólo el dueño de una llave privada puede encriptar un documento de tal forma que se pueda desencriptar con su llave pública, lo que garantiza que ha sido A y no otro el que ha enviado dicho documento.

Así mismo proporciona Integridad de datos, ya que si el documento fuera accedido y modificado en el camino el resumen del documento cambiaría también"[149]

Por último con lo anterior ya podemos ver la forma en que el notario intervendría en la firma digital y la certificación de la misma seria cuando el usuario genera con un software especial, el requerimiento de certificación y su par de claves pública y privada, el agente certificador es decir el notario verifica la personalidad, la identidad y la declaración del usuario y genera un precertificado. La autoridad certificadora verifica el precertificado, genera el certificado y lo manda a registrar con la autoridad registradora la que pide autorización a la autoridad central y registra el certificado en la base de datos enviando la notificación de registro a la autoridad certificadora quien a su vez envía el certificado ya registrado al notario para que entregue al usuario el certificado ya reconocido, el usuario recoge su certificado autentico con el notario y firma el acta notarial correspondiente, luego el usuario envía un documento con su firma electrónica y su certificado digital a un usuario receptor, quien verifica en la autoridad registradora la autenticidad del certificado y que este se encuentre en la lista de emitidos, también obtiene la clave pública del certificado y verifica la firma.

[149] MORENO, Luciano, op cit.

Como se desprende de lo anterior la seguridad tecnológica esta dada y se resuelve el problema legal ya que vemos la intervención de un tercero confiable, que es el notario quien por definición tiene todas las facultades y atributos legales para otorgar plena seguridad jurídica al procedimiento anterior.

5.2 La firma en la legislación notarial

Primero que nada hay que señalar que el Derecho Notarial es "aquella rama científica del derecho público que constituyendo un todo orgánico que sanciona en forma fehaciente las relaciones jurídicas voluntarias y extrajudiciales mediante la intervención de un funcionario que obra por delegación del poder público" [150]

Por otro lado la Ley del Notariado para el Distrito Federal en el Capítulo II que conoce De la Función Notarial y del Notariado, la Sección Segunda habla Del Notario y establece la definición del mismo en el "Artículo 42. - Notario es el profesional del Derecho investido de fe pública por el Estado, y que tiene a su cargo recibir, interpretar, redactar y dar forma legal a la voluntad de las personas que ante él acuden, y conferir autenticidad y certeza jurídicas a los actos y hechos pasados ante su fe, mediante la consignación de los mismos en instrumentos públicos de su autoría.

El notario conserva los instrumentos en el protocolo a su cargo, los reproduce y da fe de ellos. Actúa también como auxiliar de la administración de

[150] BAÑUELOS SÁNCHEZ, Froilán, *Derecho notarial*, 3ª edición, Editorial Cárdenas Editor y Distribuidor, México 1994, p 80.

justicia, como consejero, árbitro o asesor internacional, en los términos que señalen las disposiciones legales relativas."

La firma en esta legislación es de suma importancia ya que en la mayoría de los actos en los que interviene este fedatario debe de estampar su firma y sello para que ese instrumento público realizado ante su fe tenga plena validez.

La historia de la función notarial se puede reconocer junto con las transformaciones sociales y los procesos de reforma de las instituciones estatales, es decir, las adecuaciones y reformas a la función notarial han sido acordes a la evolución de las instituciones del Estado.

Ya desde la época colonial la función del notario era considerada de suma importancia para las actividades del poder público lo que llevo a que en 1792 por Cedula Real, otorgada por Carlos IV Rey de España se erigiera el Real Colegio de Escribanos de México, primer Colegio de Notarios del Continente Americano.

En la época de las Leyes de Reforma, el Imperio de Maximiliano, la Regencia Conservadora y la Presidencia Juarista se dieron momentos importantes para crear el marco jurídico que regularía a la función notarial. El 1º de febrero de 1864 la Regencia Conservadora dicto el decreto por el que se regulaba el ejercicio del notariado sustituyéndose el oficio público del escribano por el de notaria pública y al escribano por el de notario, estableciendo en él artículo 1º del Decreto que a los dueños y encargados de las notarias se les llamaría Notarios Públicos del Imperio y en la manera de habilitarse y de desempeñar sus obligaciones respectivas quedaran sujetos a lo que disponen o dispusieran las leyes.

El 21 de diciembre de 1865 se pública en el diario Oficial del Imperio el decreto que creo la Ley Orgánica del Notariado y del oficio de escribano, siendo esta reconocida como la primera ley rectora de la materia notarial.

En esta ley se distinguen al notario del escribano siendo este último el actuario del juzgado se separa a regulación de la actividad notarial respecto de la administración de justicia y sus respectivas leyes y se define al Notario en él "Artículo 1º. - El notario público es un funcionario revestido por el soberano de la fe pública para entender y autorizar las escrituras de los actos y contratos ínter vivos o mortis causa."

En contraste con el anterior artículo la Ley Orgánica de Notarios y Actuarios del Distrito Federal promulgada por el Presidente Juárez el 29 de noviembre de 1867 vino a reformar diversos contenidos sobre la función notarial que a la postre prevalecieron en diversos cuerpos normativos del notariado existentes aún a lo largo de estos años.

El Artículo 2º de dicha Ley definió al Notario como " . . . El funcionario establecido para reducir a instrumento público los actos, los contratos y últimas voluntades, en los casos que las leyes lo prevengan o lo permitan"

Entre otras disposiciones esta Ley integro el protocolo abierto a la actuación notarial; sustituyó el signo real que se empleaba por el sello de autorizar; establece el protocolo como el único instrumento donde se podía dar fe originalmente, y la atribución exclusiva de los notarios de autorizar en sus protocolos, con arreglo a las leyes, de toda clase de instrumentos públicos.

Al iniciar el siglo XX el presidente Porfirio Díaz promulgo el 19 de diciembre la Ley de Notariado de 1901; desde esta ley, el notariado es asumido

con el carácter de función pública, se dispuso que el ejercicio de la función notarial fuera de orden público, conferido por el Ejecutivo de la Unión; que la prestación del servicio notarial no causaba un sueldo proveniente del erario público; se postula la incompatibilidad del ejercicio de la función notarial con otros cargos, empleos o comisiones públicos, excepto el de la enseñanza, se prevé la separación del cargo; la existencia de aspirantes y la obtención de la respectiva patente, así como la de notario, entre otros avances que contribuyeron a delinear el perfil del notariado contemporáneo, su practica y actuación profesional.

La Ley de Porfirio Díaz fue abrogada el 20 de enero de 1932, fecha en que se público en el Diario Oficial de la Federación la Ley del Notariado para el Distrito y Territorios Federales de 1932, siendo Presidente de la República Pascual Ortiz Rubio.

Esta nueva disposición básicamente mantiene la estructura de la ley anterior, estableciendo entre otras innovaciones, una comisión del jurado de aspirantes a notario, integrándolo con cuatro notarios y un representante del Departamento del Distrito Federal, y otorgo al consejo de notarios el carácter de Órgano Consultivo de la Autoridad Administrativa Local.

Catorce años después, el 23 de febrero de 1956 se pública en el Diario Oficial de la Federación la Ley del Notariado para el Distrito Federal y Territorios de 1945, misma que mantiene al igual que sus antecesoras el carácter de función pública.

Esta ley fue la más acertada en el tratamiento de la formalidad que merece la actuación del notario, quien por cierto es el guardián de las formalidades de los actos de los particulares.

En esta ley se destaca, entre otras cosas, el delicado tratamiento del régimen de responsabilidades en que puede incurrir el notario con motivo del indebido ejercicio de sus funciones.

El 8 de enero de 1980 fue publicada en el Diario Oficial del Distrito Federal la Ley del Notariado del Distrito Federal que derogo la de 1956 manteniendo en esencia la misma estructura y el carácter de función pública buscando perfeccionar diferentes conceptos.

Pasaron casi 20 años para que este ordenamiento nuevamente fuera revisado y modificado por la Asamblea Legislativa del Distrito Federal, I legislatura, con las facultades que le otorgaba el nuevo marco jurídico de la Ciudad de México, el 30 de diciembre de 1999 aprobó la Ley de Notariado para el Distrito federal, misma que fue publicada el 28 de marzo de 2000 en la Gaceta Oficial del Distrito Federal.

Además en los órganos auxiliares de la función notarial agrega la creación del instituto del Notariado, que entre otras funciones, destaca sus propuestas de políticas públicas en materia cibernética aplicada al notariado, y la creación del decanato del Colegio de Notarios.[151]

La última reforma a este ordenamiento fue realizada por la Asamblea Legislativa del Distrito Federal, I Legislatura y fue publicada el 14 de septiembre de 2000 en la Gaceta Oficial del Distrito Federal.

En esta ocasión se modificaron un total de 21 artículos de la ley, con la finalidad de buscar mayor eficiencia notarial y una reducción en los costos de los

[151] PÉREZ FERNÁNDEZ DEL CASTILLO, Bernardo, *Apuntes para la historia del notariado en México*, Asociación nacional del notariado mexicano, México, 1979, págs 26 a 34.

servicios notariales a partir de establecer mecanismos de libre competencia, garantizando en todo momento que la función notarial mantenga su actuación en los principios de objetividad y legalidad, haciendo prevalecer en todo momento el interés general y la seguridad jurídica en beneficio de los habitantes de la Ciudad de México.

El 19 de abril de 2001 el Diputado Juan José Castillo Mota Presidente de la Mesa Directiva de la Asamblea Legislativa del Distrito Federal quien es miembro del PRD, con fundamento en el Artículo 122 Base Primera, Fracción V, inciso n, de la Constitución Política de los Estados Unidos Mexicanos, sometió a la consideración de esta Soberanía la Iniciativa del **DECRETO POR LA QUE SE ADICIONAN DIVERSOS ARTÍCULOS DE LA LEY DE NOTARIADO PARA EL DISTRITO FEDERAL,** que en su exposición de motivos comenta: "Dado la evolución de la función notarial en nuestro país ha permitido que los Notarios sean verdaderos peritos en Derecho, cuya función primordial es la de asesorar a quienes ante ellos han de formalizar un acto jurídico, a diferencia del "Notary Public" que existe en los sistemas de derecho consuetudinario o de tradición anglosajona como los Estados Unidos.

Conforme a la legislación notarial de México, su trabajo consiste en que el Notario, en virtud de su asesoría y conformación imparcial de su documentación en lo justo concreto del caso, en el marco de la equidad y el estado constitucional del derecho y de la legalidad derivada del mismo, reciba por fuerza legal el reconocimiento público y social de sus instrumentos notariales con las finalidades de protección de la seguridad jurídica de los otorgantes y solicitantes de su actividad documentadora.

La Ley del Notariado para el Distrito Federal, establece como principios regulatorios e interpretativos de la función y documentación notarial:

1. El de la conservación jurídica de fondo y forma del instrumento notarial y de su efecto adecuado;

2. El de la conservación del instrumento notarial y de la matricidad en todo tiempo del mismo;

3. El de la concepción del Notario como garantía institucional;

4. Estar al servicio del bien y la paz jurídicos de la ciudad y del respeto y cumplimiento del derecho;

5. El ejercicio de la actividad notarial, en la justa medida en que se requiera por los prestatarios del servicio, obrando con estricto apego a la legalidad aplicable al caso concreto, de manera imparcial, preventiva, voluntaria y auxiliar de la administración de justicia, respecto de asuntos en que no haya contienda, mantendrá siempre una actitud de ulteralteridad.[152]

6. El del cuidado del carácter de orden público de la función y su documentación en virtud del otorgamiento de la calidad para dar fe, por el Jefe del Gobierno, a su actividad como Notario por la expedición de la patente respectiva, previos exámenes que merezcan tal reconocimiento público y social por acreditar el saber prudencial y la practica suficientes para dicha función, con la consecuente

[152] Deontología “actitud un procedimiento de asesoría notarial y de conformación del instrumento notarial que va mas allá de un a simple imparcialidad, llevando al Notario a ser un verdadero consultor o consejero de cada parte, con atención personal y entrega cuidadosa, de forma tal que se cubran los requisitos de asesoría y consejo para cada una de las partes o solicitantes del servicio, sin descuidar los de la contraparte, ni ser parcial contra ella, sino ejerciendo hacia ella la misma actitud, basada en lo justo concreto del caso de que se trate”. PÉREZ FERNÁNDEZ DEL CASTILLO, Bernardo, *Deontología Jurídica, Ética del Abogado,* Editorial Porrua, México 1997, págs 139-145

pertenencia al Colegio y la coadyuvancia de este a las funciones disciplinarias de vigilancia y sanción por parte de las autoridades, la continuación del archivo del Notario por el archivo y la calificación y registro de los documentos públicos reconocidos por esta Ley, y por el Registro Público, tratándose de actos inscribibles." [153]

Con la iniciativa se intenta reforzar la necesaria e indispensable actividad del notariado del Distrito Federal a través de medios electrónicos, actualizándola a fin de que este acorde con las reformas y disposiciones que en otros ordenamientos fundamentalmente de carácter federal se han hecho para que la comunicación remota o la contratación por vía electrónica, sea jurídicamente segura ejemplo de esto lo encontramos en el Capítulo II de este trabajo donde ya se ha mencionado el trato que en diversos cuerpos normativos de nuestro país.

Podemos decir que mediante las reformas tanto civiles, mercantiles y procésales, se estableció la posibilidad de que dos personas puedan validamente manifestar su consentimiento para obligarse, mediante cualquier medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de esta en forma inmediata, y estos se, tendrán por cumplidos, siempre que la información generada o comunicada en forma integra, a través de dichos medios, sea atribuible a las personas obligadas y accesibles para su ulterior consulta en la función notarial.

Por último derivado de la anterior iniciativa de decreto por que se propone adicionar diversos artículos de la Ley del Notariado para el Distrito Federal

---

[153] TORRES BALTAZAR, Edgar, *Decreto por el que se adicionan diversos artículos a la ley de notariado para el Distrito Federal*, Diputado, Asamblea legislativa del Distrito Federal, II Legislatura, págs 4 a 14.

presentada por el Diputado Edgar Torres Baltazar, la Asamblea Legislativa a través de las Comisiones Unidas de Notariado y Ciencia, Tecnología e Informática, emitió el dictamen sobre tal iniciativa, dicho dictamen tomo en cuenta los antecedentes de la iniciativa de decreto, así que el Pleno de la Honorable Asamblea Legislativa hizo las siguientes consideraciones de importancia:

a) Es de sumo interés de la Comisión de Notariado buscar los elementos que tiendan a evolucionar la labor notarial, conservando su función autenticadora, la que hasta hoy le ha valido el reconocimiento público y social en relación con los instrumentos notariales que emite, dada la legalidad, certeza y seguridad jurídica de la que los reviste.

b) La Comisión de Ciencia, Tecnología e Informática sabe de lo importante del desarrollo tecnológico para adecuar los instrumentos jurídicos y en este caso la ley del Notariado para el Distrito Federal.

c) El uso de la firma electrónica como sustitución de la firma autógrafa no es posible garantizarla, como si estuviéramos en el supuesto de que un asaltante usara él numero confidencial el que equivale a la firma electrónica de la persona asaltada sin ser el quien tiene derecho a usarla; o como sabemos la computadora donde se guarda la firma electrónica no es un sitio 100% seguro, pues un hacker podría copiarla y utilizarla en perjuicio de su dueño, ya que en la practica una computadora es usada por varias personas.

d) La firma electrónica no muere simultáneamente con el dueño de la firma autógrafa, personas interesadas podrían levar a cabo operaciones que requieran de fe pública, sin la voluntad del sujeto fallecido, durante el periodo que transcurre entre la muerte del sujeto y la notificación del Registro Civil al notario.

e) Las transacciones bursátiles y bancarias que utilizan firma o identificadores electrónicos se llevan a cabo sobre redes especiales más seguras que el Internet, la cual es una red poco segura para la función notarial.

f) Sin consideraciones cuidadosas técnicas y detalladas, se pretende elevar el nivel jurídico de los identificadores digitales concebidos para el cruce de correros electrónicos entre entidades privadas y constituir a los notarios en agentes certificadores de claves públicas y privadas en sustitución de entidades independientes emisoras de certificados.

g) El sello notarial en la historia del notariado latino ha sido considerado como un elemento más para garantizar la autenticidad de los documentos que lo llevan. En al Propuesta del Diputado Torres se hace una referencia imprecisa y ambigua respecto del sello ". . . sello electrónico, óptico o de cualquier otra tecnología que garantice la equidad jurídica y tecnológica", esta referencia no es una especificación precisa de lo que debe ser un sello electrónico notarial, ese es un cabo suelto que de desprende de dicha iniciativa de decreto, al igual que al mencionar al protocolo.[154]

Del Dictamen que estamos comentado se desprendieron los siguientes considerandos; se tiene que ajustar el trabajo notarial al desarrollo tecnológico, aunque sin olvidar que la tecnología no es perfecta, y que se debe de poner especial atención a la seguridad tecnológica que de debe brindar a los usuarios, este Dictamen también consideró que la propuesta del Diputado Torres es una

---

[154] RAMOS ITURBIDE, Bernardino, et al, Presidente de la Comisión del Notariado, *"Dictamen sobre la iniciativa de Decreto por el que se propone adicionar diversos artículos a la Ley del Notariado para el Distrito Federal",* México D.F. 20 de marzo de 2003, págs 1 a 6

oportunidad para impulsar la función notarial en nuestro país, lo que lo colocaría en el mundo cibernético, el que día a día se transforma, con lo cual debemos poner cuidado para precisar elementos que son fundamentales en la función del Notario.

A pesar de que se desecho la iniciativa propuesta por el Diputado Torres, es una buena propuesta para tratar de llevar a México a primer plano en materia notarial, esta como dije de desecho por que no garantizaba la vinculación legal de la identidad del sujeto con su firma digital, tampoco garantiza la no-duplicidad de claves públicas y privadas, tampoco garantiza que la difusión de las claves públicas a través de Internet sea siempre sin alteraciones de ellas en el proceso, y los elementos como sello, protocolo, apéndice e índice electrónico, óptico o de cualquier tecnología son ambiguos y aún no aportan certeza jurídica que esta demandando la sociedad, en franca violación a los principios regulatorios e interpretativos de la función notarial.

Como se puede desprender de lo anterior, cada día se hace más necesaria la intervención del notario. Debidamente actualizado en materia informática en las transacciones vía electrónica, el ámbito laboral del notario no cesa, si no al contrario cada vez va encontrando más nichos en los cuales su intervención más que ser necesaria es indispensable.

En el Distrito Federal, el notariado esta proponiendo reformas que incluyan los anteriores conceptos a la legislación, lo que hará en caso de ser aceptadas por la Asamblea Legislativa, que la Ley del Notariado para el Distrito Federal sea la primera en contemplar al Notario Electrónico (Cybernotario).

5.3 Proyecto de Cybernotario

Esta figura tiene su origen en Estados Unidos de Norteamérica, desde que la American Bar Association, dío a conocer en 1996, los trabajos alrededor del proyecto del Cybernotario, estos trabajos han buscado que dicha figura se constituya un tipo de oficial que brinde seguridad y que además combina la experiencia técnica y legal con la competencia para intervenir en transacciones casi de todo tipo; dado que las funciones que los fedatarios públicos pueden ejercer en el mundo virtual, no son diversas de las que hoy ejercen en el mundo real.

El objetivo primordial del proyecto de la American Bar Association, fue el de eliminar la carencia de obligatoriedad de los actos celebrados en ese país para que tengan plenos efectos legales en otros países; es decir dicho proyecto se ideo para que los actos pasados ante el Cybernotario tuvieran pleno reconocimiento y efectos fuera de Estados Unidos, debido a que dicho profesional será un obligado común del Common Law, cuyas funciones se asemejan a las de un Notario de un país basado en el Civil Law y todo eso para construir un puente entre 2 tradiciones legales asegurando que las transacciones en las que intervenga el notario moderno reunirán los requisitos de procedimiento y formalidades requeridas por las jurisdicciones que se basan tanto en el derecho común como en el civil. [155]

A pesar que en Estados Unidos de Norte América, existe la figura del notario, esta tiene diferencias respecto del notario latino, mientras que el notario

[155] DEVOTO, Mauricio y M. LYNCH, Horacio, Banca, Comercio, Moneda Electrónica y Firma Digital, Proyecto Cybernotario, Publicaciones CENIT, [En línea]. Disponible: http://www.it-cenit.org.ar/Publicac/BancaMD/BanCom5, 15 abril de 2006.

anglosajón, es un particular; su cargo es temporal; no cuenta con estudios jurídicos; no redacta ni es el autor del documento; su documento no hace prueba; no da forma a los contratos y no expide copias autenticas; y el notario latino a contrario sensu si es un abogado; un cargo permanente; es un experto en derecho redacta y el es autor del documento; su documento si hace prueba plena; da forma a los contratos; conserva los documentos y si puede expedir copias autenticas.[156]

Dado lo anterior el Cybernotario busca actuar en forma similar al notario latino; es decir es un abogado pare proviene de la rama Romano-Germánica que tiene un alto grado de fiabilidad y de responsabilidad en cierto tipo de operaciones como escrituras, certificar transacciones, constituir sociedades, elaborara testamentos, dar constancia de una fe de hechos etc; siendo entonces de suma importancia la capacidad para certificar y autenticar electrónicamente por parte del Cybernotario.

El Cybernotario cumple con 2 funciones básicas:

a) Realiza una investigación de los usuarios que quieran registrar sus claves públicas para su uso en el comercio electrónico principalmente ya que la política y procedimientos para su registro serán establecidos por la autoridad certificante, en este sentido el Cybernotario funciona como una compuerta de seguridad para los usuarios de la tecnología.

b) Interviene en las transacciones de derecho comercial internacional así que el Cybernotario proveerá certificación y autenticación independientemente del proceso de acreditación al que las partes hayan debido someterse para

---

[156] GÓMEZ-MARTINHO FAERNA, Augusto, *La función del notario en la Unión Europea: un estudio comparativo,* Editorial Junta de Decanos de los Colegios Notariales de España, España, 1997, p 105.

obtener sus claves públicas, su tarea principal consiste en determinar la capacidad del usuario para realizar la transacción de que se trate, así como la verificación de todos los aspectos legales relacionados con la transacción en si misma, lo anterior determinara si la transacción cumple o no con los requisitos de forma y fondo de la jurisdicción que le corresponde.

En Estados Unidos mediante el uso de la firma digital el llamado Cybernotario podrá certificar, la identidad del emisor de un mensaje, dar un nivel de seguridad en cuanto al contenido del mismo, fechar la notarización, es decir asentar la fecha y hora de su intervención y su respectiva protocolización, por lo tanto, el actuar electrónico del Cybernotario, se realiza por medio de mecanismos electrónicos, es decir las certificaciones electrónicas se hacen mediante una firma digital.

Ahora bien una certificación electrónica es un mensaje adjuntado al que esta siendo certificado, el efecto de tal certificación es similar a la que se hace en papel, es decir se pueden expedir copias certificadas de documentos, sí como él Cybernotario puede expedir copias certificadas de los mensajes de datos.[157]

En nuestro país ya contamos con profesionales que ejercen la función pública de ser fedatarios electrónicos, los cuales solo necesitan acreditar sus conocimientos tecnológicos, capacidad humana y solvencia técnica como para fungir como certificadores electrónicos.

---

[157] PERALES SANZ, José Luis, *La seguridad jurídica en las transacciones electrónicas*; seminario organizado por el consejo general del notariado en la UIMP, Coedición Civitas Ediciones, España, 2002, p 250.

Al respecto la empresa denominada ACERITA, ha implementado una propuesta con distintas Asociaciones y Colegios de Notarios y Corredores Públicos tanto de América Latina como de España para que puedan implantar elementos tecnológicos y la infraestructura necesaria para iniciar operaciones como Cybernotario.

Tal infraestructura necesaria para la practica del comercio electrónico seguro tiene ciertos componentes tecnológicos y jurídicos, los primeros relacionados con la aplicación de la tecnología de encriptación y con el uso de su estructura administrativa conocida como PKI Public Key Infraestructure, tema que ya abordamos en el capítulo que antecede, y los segundos relacionados con el nivel de legalidad que aportan quienes participan en los procesos de certificación.

5.3.1 Acertia

Dadas las funciones desarrolladas por los participantes de la PKI y la estructura de legalidad requerida ACERITA ha llegado a considerar que la entidad más indicada para tener el carácter de certificador digital es la del fedatario público, es por eso que según la infraestructura implementada por Acerita y puesta a disposición de Fedatarios Públicos esta orientada a cumplir con 3 clases de infraestructura:

1.- Tecnológica, con software y hardware para cada autoridad certificadora y correspondientes agentes certificadores;

2.- Servicios, capacitar, investigar y desarrollar para cumplir con la actualización e inversión en nuevas tecnologías y aplicaciones para los fedatarios públicos; y

3.- Comercial.- operación, administración y desarrollar alianzas para aumentar la infraestructura de las autoridades certificadoras y de registro de los fedatarios públicos y los fedatarios mismos.

El papel que juega la empresa Acerita, es el de autoridad certificadora en si misma y como operadora de las autoridades certificadoras de Notarios y Corredores públicos, ya que ambos son el sustento de legalidad en proceso de certificación digital y tienen la posibilidad de trasladar al mundo virtual el valor de la fe pública que ejercen en el mundo terrenal.

Bueno digamos que las funciones tanto, de los fedatarios públicos como Acerita se entrelazan de tal manera que se puede llegar finalmente a la certificación digital; es decir, de una primera parte los fedatarios prestan el servicio 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; y de una segunda parte Acerita pondrá a su disposición de los fedatarios las aplicaciones necesarias para implantar el protocolo electrónico en la medida en que las disposiciones legales hagan necesaria su intervención en los actos que se puedan realizar vía electrónica.

Como mencionamos en nuestro país ya existen notarios públicos; llamados agentes certificadores de Acerita, los cuales para disponer de una firma digital siguieron los siguientes pasos.

a).- Generación de claves, primero se obtiene un software generador de requerimientos de certificación digital, en la sección de documentos de la pagina web de Acerita, se ejecuta en la computadora el programa y captura los datos que se soliciten, se graba en un disquete el requerimiento de certificación e imprimir la solicitud de certificación digital y ya con los documentos correspondientes acudir a un agente certificador es decir en este caso el notario;

b).- Certificación y registro de la clave pública, donde el agente certificador llámese notario, verifica los documentos y requerimiento de certificación, da fe de la identidad del solicitante así genera su certificado digital y lo registrará ante la autoridad que corresponda;

c).- Uso de la firma digital el agente certificador es decir el notario entrega el certificado digital en un medio magnético y conserva el testimonio del acta donde constan los hechos y declaraciones pasadas ante su fe, por lo que por último restaría instalar en la computadora el certificado digital, el que permitirá usarlo para firmar digitalmente en las transacciones comerciales.

El servicio que presta Acerita, es en cierta forma innovadora, ya que es una de las primeras en crear una estructura para que el Notario sea agente certificador, sin embargo uno de los problemas de tipo practico es el de costear la infraestructura que se requiere para operar este tipo de cuestiones; ya que para algunos de los usuarios implicaría un gasto fuerte si tomamos en cuenta que un certificado digital se comercializa aproximadamente en 600 dólares, y poca gente estaría dispuesta a invertir esa cantidad.

5.4 Escritura Pública

Primero que nada y de acuerdo a la Ley del Notariado, para el Distrito Federal en el Capítulo II. De la Actuación Notarial, Sección Tercera De las Actuaciones y Documentos Notariales, alude a las escrituras:

"**Artículo 100.** - Escritura es cualquiera de los instrumentos públicos siguientes:

I.- El original que el notario asienta en folios, para hacer constar uno o más actos jurídicos y que firmado por los comparecientes, el Notario autoriza con su sello y con su firma;

II.- El original integrado por lo siguiente:

a) Por el documento en el que el Notario consigna uno o más actos jurídicos y que deberá llenar las formalidades que este capítulo establece; ser firmado en cada una de sus hojas y al final por los comparecientes y el Notario; llevar el sello de éste en los expresados lugares y agregarse al apéndice con sus anexos. Hará mención de la escritura de la que forma parte y el o los folios en los que se contiene la síntesis a que se refiere el inciso siguiente y,

Por la síntesis asentada por el Notario en los folios que correspondan, en la que se señalen los elementos personales y materiales del o de los actos consignados. Dicha síntesis contendrá el número de hojas de que se compone así como una relación completa de sus anexos, y una vez firmada por los comparecientes será autorizada por el Notario con su sello y firma."

Es importante mencionar que al referirnos a una escritura pública, en el mundo real, su equivalente en el mundo virtual seria un instrumento o documento informático los cuales tendrían las mismas solemnidades exigidas por la ley para la celebración de contratos y actos jurídicos por lo tanto ambos como instrumentos, realizados por notario público gozaran de fehaciencia e individualidad debiendo ser confeccionados de acuerdo a la ley sin que pudieran adolecer de causales de nulidad.

Ahora bien si equiparamos una escritura con un documento electrónico, en ambos deben concurrir los siguientes requisitos y deberes por parte del notario para su celebración:

1.- Lenguaje y estilo.- con el debido tecnicismo pero hacerlo entendible para las partes que intervienen;

2.- Enmienda y corrección de errores.- donde el notario hace las observaciones que considere y en dado caso hacer las correcciones que le fueran observadas por las partes que intervienen así entonces si hubiere correcciones o errores serán subsanados estas ultimas y salvadas de la manera usual;

3.- Rogación.- esto el requerimiento que consiste en la interposición del ministerio notarial o instancia de parte interesada, la rogación viene de la palabra rogatio proveniente del Charta Romana que surge a partir de Justiniano en donde la rogatio no constituiría un simple formulismo sino que produciría efectos jurídicos; entonces la rogatio es una petición solemne hecha por el autor al notario a objeto de que este interviniese como suscriptor del documento.”

4.- Partes de una escritura que consta de:

- Comparecencia e individualización, primer contacto que tiene el fedatario con la parte interesada, es el primer paso a observar en una escritura en la que se determina el acto que constituye su objeto y las personas que constituirán la relación actual o contractual, es decir es la comparecencia física de las partes actuantes ante el notario;

- Parte expositiva o descriptiva, es la parte que describe los inmuebles, la presentación de documentos, relación de títulos de adquisición inmuebles y designación de cargas o gravámenes, esta parte de la escritura es donde se hace la descripción del objeto de la relación instrumental o del concurso de voluntades, estableciendo además lo que servirán de antecedentes necesarios para los pactos, estipulaciones o manifestaciones de voluntad, por lo tanto en esta parte de la escritura quedan fijados el objeto de la escritura pública, su causa y antecedentes que sirven de expresión al objeto;

- Parte dispositiva o estipulatoría también llamada como la parte contractual y la que debe ser redactada de acuerdo con la voluntad de los otorgantes o con los pactos o convenios acordados por las partes que intervienen en la escritura, así el notario cuida reflejar con la debida claridad y separadamente los que se refieren a cada uno de los derechos creados, transmitidos, modificados o extinguidos, y adicionalmente debe de cuidad el alcance de las facultades determinables y obligaciones de cada otorgante o tercero a quienes pudiera afectar el documento.

Ahora bien por último las cláusulas estipulatorias son las que contienen las declaraciones de voluntad propias del acto o contrato y formulan expresiones de voluntad jurídica que vinculan absolutamente a las partes, reduciendo a partir de ellas efectos declarativos y ejecutivos plenos.

- Cumplimiento de deberes notariales que emanan de las estipulaciones, en el proceso de materialización es decir en la confección o formalización de la escritura pública, el notario y ya no las partes debe a su vez cumplir con una gama de deberes que importan verdaderos principios atingentes a su calidad de autor de esta, todo lo cual ha de hacerse en virtud de la eficacia y seguridad jurídica que importa la proporción de la autorización de la misma, los deberes del notario se resumen a 5 puntos:

Principio de autoría y de responsabilidad ya que el notario como autor del documento tiene obligaciones que emanan de tal condición, es decir tiene la obligación de asesorar a las partes; tal función implica también que el notario informe a las partes acerca de la normativa jurídica aplicable a la relación querida por ellas, procediendo luego a efectuar la labor formativa del acto o contrato, es decir a la redacción, para lo cual se ciñe con toda fidelidad a las instrucciones que le hayan sido dadas, informándoles además el valor y alcance legal de su redacción. [158]

Control de legalidad, bajo el cual obliga primero al notario a precaver la naturaleza jurídica del instrumento público al señalar que este es el autorizado con las solemnidades legales por el competente funcionario; y segundo, este control de legalidad se ejerce del mismo modo por el notario en relación con su función asesora, a quién les aconseja, los medios jurídicos más adecuados para el logro de los fines lícitos que las partes quieren alcanzar, así el notario esta obligado a velar por el cumplimiento de todos los requisitos establecidos por ley respeto del

[158] GAETE GONZÁLEZ, Eugenio Alberto, op cit, p 306.

acto o contrato u objeto de que este sea plenamente válido y nazca a la vida jurídica sin vicios que lo invaliden.[159]

Deber de imparcialidad, es uno de los principios más importantes que guían al notario, y que conjuntamente con el principio de la legalidad, producen confianza a las partes, es decir el notario no puede aconsejar ni procurar ventajas para alguna de las partes.[160]

Principio de intermediación, por este el notario debe estar, en contacto con las partes que intervienen en la escritura pudiendo dar fe solo de aquello que ocurre que tiene lugar en su presencia y por ende percibe por sus sentidos.

Deber de conservación del documento, este deber es muy importante ya que tiene por objeto, el formar el protocolo con el objeto de mantener los originales; el de otorgar copias de los originales; el de otorgar seguridad jurídica al instrumento asegurado, su manutención por medio de su guarda y conservación evitando su pérdida, ocultación o falsificación; y por último desde el punto de vista del Estado a este le interesa la manutención, de los protocolos, en cuanto a través de estos es posible reconstruir algún hecho pasado ante su fé; en atención a lo anterior el notario debe ir constituyendo el protocolo, en donde se encuentran el conjunto de escrituras públicas pasadas ante su fé, el cual queda en su custodia.

Otorgamiento de escritura pública, es la forma documental que reviste la audiencia, es decir en audiencias es el objeto y el otorgamiento la forma, ahora bien el otorgamiento esta constituido por varios pasos que el notario debe cumplir

---

[159] DE PRADA, José Maria, *La forma de los actos jurídicos privados y la seguridad jurídica*., Consejo Nacional del Notariado, Universidad Internacional Menéndez Pelayo, Impresión en México, Madrid 1990, p 103.
[160] GAETE GONZÁLEZ, Eugenio Alberto, op cit, p 308.

en la audiencia, como reserva y advertencia legales lectura del documento, el enterado de los comparecientes, conformidad de estos con el texto o consentimiento y firma de los interesados.

Autorización de la escritura es el suscribir por el notario que ha intervenido en la audiencia es el último paso donde se determina que se han cumplido con todas las etapas por los que el acto, ha debido pasar. [161]

Así el notario queda obligado asignar, firmar, rubricar y sellar el documento para que las autorizaciones tengan valor en el caso del instrumento público electrónico el otorgamiento y la autorización instrumental adquieren la misma importancia, que si se hiciera en papel, en cuanto del cumplimento preciso de las solemnidades instrumentales derivara el carácter público de éste.

En el Decreto por el que se adicionan diversos artículos de la Ley del Notariado para el Distrito Federal. , y al que ya aludimos anteriormente menciona conceptos relacionados con las escrituras como:

> **“ DE LAS ACTAS.**
>
> **Artículo 125 bis**.- Acta notarial también es el documento electrónico, en donde conste que el Notario generó, envió, recibió, comunicó, archivo o autorizó en forma íntegra una escritura o acta elaborándolo mediante los medios electrónicos ópticos o de cualquier otra tecnología, asegurándose que dicha información es atribuible a las personas obligadas y esta se mantiene accesible para su ulterior consulta.

[161] Ídem.

DE LOS TESTIMONIOS

Artículo 143 bis.- También es testimonio el documento electrónico, en donde conste que el notario, generó, envió, recibió, comunicó, archivo o autorizó en forma íntegra una escritura o acta elaborándola mediante los medios electrónicos, ópticos o de cualquier otra tecnología asegurándose que dicha información es atribuible a las personas obligadas y esta se mantiene accesible para su ulterior consulta".[162]

En todos los casos el notario deberá observar todas y cada una de las formalidades, para la elaboración del documento notarial, que se señalen en la presente ley.

5.5 Protocolo electrónico.

De acuerdo a la Ley del Notariado para el Distrito Federal, en el Artículo 76 se define al protocolo notarial como: "Protocolo es el conjunto de libros formados por folios numerados y sellados en los que el notario, observando las formalidades que establece la presente Ley, asienta y autoriza las escrituras y actas que se otorguen ante su fe, con sus respectivos apéndices; así como por los libros de registro de cotejos con sus apéndices.

En sentido amplio es la expresión que se refiere a todos los documentos que obran en él haber de cada notaría. El protocolo es abierto, por cuanto lo forman folios encuadernables con número progresivo de instrumentos y de libros. En sentido estricto es tanto el conjunto de instrumentos públicos fuente original o

[162] TORRES BALTAZAR, Edgar, op cit, págs 4 a 14.

matriz en los que se hace constar las relaciones jurídicas constituidas por los interesados, bajo la fe notarial; como la colección ordenada cronológicamente de escrituras y actas autorizadas por el Notario y aquellas que no pasaron, y de sus respectivos apéndices, conforme a una periodicidad, procedimiento y formalidades reglados en esta Ley; y que adquiridos a costa del Notario respectivo son conservados permanentemente por él o por su sustituto en términos de esta Ley afectos exclusivamente al fin encomendado y, posteriormente, destinados permanentemente al servicio y matricidad notarial del documento en el Archivo como propiedad del Estado, a partir de la entrega de los mismos a dicha oficina, en uno o más libros, observando para su redacción y conformación de actos y hechos las formalidades y solemnidades previstas por esta Ley, todo lo que constituye materia de garantía institucional de origen constitucional regulada por esta Ley.

Los folios que forman el protocolo son aquellas hojas que constituyen la papelería oficial que el notario usa para ejercer la función notarial. Son el fundamento o base material del instrumento público notarial, en términos de esta Ley." [163]

Ahora bien en el mismo Decreto ya aludido antes se refiere al protocolo electrónico y lo define en el Artículo 76 bis como: "Protocolo electrónico es el conjunto de medios electrónicos ópticos o de cualquier otra tecnología mediante los que el Notario observando las formalidades, que establece la presente ley, podrá, generar, enviar, recibir, comunicar, archivar o autorizar en forma íntegra los hechos y actos jurídicos que se otorguen ante su fé, asegurándose que dicha

[163] Ídem.

información es atribuible a las personas obligadas por esta se mantiene accesible para su ulterior consulta, en cuyo caso el notario deberá hacer constar en el propio instrumento electrónico, los elementos a través de las cuales se atribuye ese hecho o acto jurídico a la o las partes conservando siempre bajo su resguardo una versión integra de la misma para su ulterior consulta otorgando dicho instrumento en los términos establecidos en la presente ley.

Para la formación del apéndice electrónico y del índice electrónico, el notario podrá utilizar, cualquier medio electrónico, óptico o de cualquier otra tecnología, que garantice que dicha información es atribuible a las personas obligadas y esta se mantiene accesible para su ulterior consulta.

En cualquier caso en que el notario, genere, envié, reciba, comunique, archive hechos y actos jurídicos que se otorguen ante su fé, éste y las partes firmaran; sellaran y lo encriptaran electrónicamente la información que sea atribuible a las personas obligadas con métodos seguros que garanticen la seguridad tecnológica y jurídica de dicha información de conformidad con las leyes y con los criterios establecidos, para ello por el Colegio de Notarios del Distrito Federal.

En termino que esta relacionado con el protocolo el mismo Decreto al que aludimos, también hace referencia al sello de autorizar, en el Artículo 75 bis “el notario podrá ejercer su facultad fedataria mediante un sello electrónico, óptico o de cualquier tecnología que garantice la seguridad jurídica y tecnología, cuando se

requiera su intervención en el ámbito electrónico de conformidad, con los criterios y bases que establezca el Colegio".[164]

5.6 Instituciones de las que se apoya el notario

5.6.1 Archivo General de Notarias.

Es de suma importancia tomar en cuenta el sistema de archivo electrónico que debe llevar por una parte el Notario Público y por la otra el Archivo General de Notarías, de las escrituras que sean pasadas ante la fé del primero; sabemos que el tipo de información que el notario maneja tiene el carácter de ser pública por los que esta debe de estar a disposición de los interesados y no puede ser reservada, algo similar pasa en el Archivo General de Notarias, que archiva la información con el mismo carácter que el Fedatario.

La existencia de un protocolo electrónico importa a su vez la necesaria intervención técnica de terceros diferentes a la autoridad certificadora, esto es al notario, así será el tercero proveedor de servicios quién los brinde, poniendo a su disposición de la autoridad certificadora entre otros servicios un sistema de archivo protocolar; para que posteriormente, se puedan otorgar copias instrumentales, a quién las solicite; la diferencia solo será que en este caso las copias serán informáticas y no mediante papel.[165]

---

[164] Ídem.
[165] GAETE GONZÁLEZ, Eugenio Alberto, op cit, p 338.

En la propuesta que se plantea en este trabajo, el Archivo General de Notarías debiera contar con un archivo electrónico de datos, contando con los elementos de seguridad tales como hardware y software, que garantice la durabilidad, inalterabilidad e inaccesibilidad de los medios de archivo, claro esta que solo para personas que tengan un interés jurídico o sean parte en el acto jurídico, la información estaría a su disposición.

El archivo tendrá un papel importante en la conservación de los datos, sería una especie de tercero proveedor de servicios, el cual mantendría la información accesible para posterior consulta, conservaría el mensaje de datos en el formato original en el cual se generó, envió o recibió o con algún formato que sea demostrable, que reproduce con exactitud la información generada, enviada o recibida y que se conserve todo dato que permita determinar el origen y destino del mensaje.

Considero que tanto el notario como el archivo, tienen sus funciones bien definidas, y no se trata de equiparar sus actuaciones, al referirnos al archivo como una 3ª parte proveedor de servicios de certificación; teniendo entonces el notario, la función de autenticar y certificar las actuaciones que se realicen ante su fé y el archivo deberá contar con un soporte suficientemente seguro y por ende durable e inalterable, que permita contener la información debidamente encriptada a través de una especie de biblioteca organizada, una recuperación direccionable de datos cuya certificación y conservación se encuentre a cargo de la autoridad certificadora correspondiente; que técnicamente sea previsto a través del proveedor de servicios o directamente por la autoridad certificadora y mediante el

cual se puedan emitir copias electrónicas de los documentos, que se encuentran bajo su custodia.

Ahora solo consideremos que el uso de la tecnología en el Archivo no garantiza, que careciéramos de riegos provenientes de casos fortuitos o de causas accidentales, para esto el archivo tendría que hacer durables sus soportes, mantenerlos al día es decir, actualizados, en cuanto a su técnica; mantener sus matrices u originales de documentos informáticos con fuertes medidas de seguridad con optimización de los soportes de su durabilidad e inalterabilidad, para que a través de ellas se puedan obtener, las copias o consultas, que se puedan requerir.

Por último todo sistema de archivo deberá estar organizado y así como el instrumento público en soporte de papel, considera una sistematización basada en el libro protocolo cuya guarda y conservación será a cargo del Notario para posteriormente de 5 años, porque así lo marca la ley, sea remitido al Archivo General de Notarías; ya que en el ejercicio de la función de Fedatario lo deja sujeto a una serie de deberes y responsabilidades que debe cumplir con el objeto de la seguridad de tales libros, de igual forma al Archivo debe contar con elementos normativos, que permitan la existencia de un sistema de archivo seguro y útil en su consulta.

5.6.2 Registro Público de la Propiedad y de Comercio y de Patrimonio del Inmueble Federal.

En el Reglamento del Registro Público de la Propiedad en el Artículo 1º dice que este es "La institución mediante la cual el gobierno del Distrito federal proporciona el servicio de dar publicidad a los actos jurídicos que, conforme a la Ley precisan de este requisito para surtidor efectos ante terceros"

Y es aquí donde se inscriben los actos mercantiles, así como aquellos que se relacionan con los comerciantes y que conforme a la legislación lo requieran. La inscripción en el Registro es potestativa, para comerciantes individuales y obligatoria, para comerciantes colectivos.[166]

Existe un proyecto impulsado por la Secretaría de Economía junto con la Asociación de Banqueros y la Asociación del Notariado, para modernizar las oficinas de los Registros Públicos y del Comercio, a escala nacional a efecto de que todos los actos jurídicos, contratos y demás constancias relacionadas con sociedades mercantiles, los asientos correspondientes se realicen en forma electrónica a través de Internet.

Por último veamos que la Secretaria de Comercio y Fomento Industrial mediante la Reforma de mayo de 2000 de la cual hemos venido haciendo alusión, en su Artículo Tercero se reforman artículos del Código de Comercio, que se encuentran ligados con la forma de operar del Registro Público y del Comercio, la cual queda como sigue:

---

[166] MANTILLA MOLINA, Roberto, *Derecho Mercantil*, 29ª Edición, Editorial Porrua, México 2000, págs 137 a 138.

” . . . ARTÍCULO TERCERO.-

Se reforman los artículos 18, 20, 21 párrafo primero, 22, 23, 24, 25, 26, 27, 30, 31, 32, 49, 80 y 1205, y se adicionan los artículos 20 bis, 21 bis, 21 bis 1, 30 bis, 30 bis 1 y 32 bis 1298-A; el Titulo II que se denominara "Del Comercio Electrónico", que comprenderá los artículos 89 a 94, y se modifica la denominación del Libro Segundo del Código de Comercio, disposiciones todas del referido Código de Comercio, para quedar como sigue:

Artículo 18.- En el Registro Público de Comercio se inscriben los actos mercantiles, así como aquellos que se relacionan con los comerciantes y que conforme a la legislación lo requieran. La operación del Registro Público de Comercio esta a cargo de la Secretaria de Comercio y Fomento Industrial, en adelante la Secretaria, y de las autoridades responsables del registro público de la propiedad en los estados y en el Distrito Federal, en términos de este Código y de los convenios de coordinación que se suscriban conforme a lo dispuesto por el artículo 116 de la Constitución Política de los Estados Unidos Mexicanos. Para estos efectos existirán las oficinas del Registro Público de Comercio en cada entidad federativa que demande el trafico mercantil. La Secretaria emitirá los lineamientos necesarios para la adecuada operación del Registro Público de Comercio, que deberán publicarse en el Diario Oficial de la Federaciones.

Artículo 20.- El Registro Público de Comercio operara con un programa informático y con una base de datos central interconectada con las

bases de datos de sus oficinas ubicadas en las entidades federativas. Las bases de datos contaran con al menos un respaldo electrónico. Mediante el programa informático se realizara la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral. Las bases de datos del Registro Público de Comercio en las entidades federativas se integraran con el conjunto de la información incorporada por medio del programa informático de cada inscripción o anotación de los actos mercantiles inscribibles, y la base de datos central con la información que los responsables del Registro incorporen en las bases de datos ubicadas en las entidades federativas. El programa informático será establecido por la Secretaria. Dicho programa y las bases de datos del Registro Público de Comercio, serán propiedad del Gobierno Federal. En caso de existir discrepancia o presunción de alteración de la información del Registro Público de Comercio contenida en la base de datos de alguna entidad federativa, o sobre cualquier otro respaldo que hubiere, prevalecerá la información registrada en la base de datos central, salvo prueba en contrario. La Secretaria establecerá los formatos, que serán de libre reproducción, así como los datos, requisitos y demás información necesaria para llevar a cabo las inscripciones, anotaciones y avisos a que se refiere el presente Capítulo. Lo anterior deberá publicarse en el Diario Oficial de la Federaciones.

Artículo 20 bis.- Los responsables de las oficinas del Registro Público de Comercio tendrán las atribuciones siguientes:

I.- Aplicar las disposiciones del presente Capítulo en el ámbito de la entidad federativa correspondiente;

II.- Ser depositario de la fe pública registral mercantil, para cuyo ejercicio se auxiliará de los registradores de la oficina a su cargo;

III.- Dirigir y coordinar las funciones y actividades de las unidades administrativas a su cargo para que cumplan con lo previsto en este Código, el reglamento respectivo y los lineamientos que emita la Secretaria;

IV.- Permitir la consulta de los asientos regístrales que obren en el Registro, así como expedir las certificaciones que le soliciten;

V.- Operar el programa informático del sistema registral automatizado en la oficina a su cargo, conforme a lo previsto en este Capítulo, el reglamento respectivo y en los lineamientos que emita la Secretaria;

VI.- Proporcionar facilidades a la Secretaria para vigilar la adecuada operación del Registro Público de Comercio, y

VII.- Las demás que se señalen en el presente Capítulo y su reglamento.

Artículo 21.- Existirá un folio electrónico por cada comerciante o sociedad, en el que se anotaran: I a XIX.- . . .

Artículo 21 bis.- El procedimiento para la inscripción de actos mercantiles en el Registro Público de Comercio se sujetara a las bases siguientes:

I.- Será automatizado y estará sujeto a plazos máximos de respuesta;

II.- Constara de las fases de: a) Recepción, física o electrónica de una forma personificada, acompañada del instrumento en el que conste el acto a inscribir, pago de los derechos, generación de una boleta de ingreso y del numero de control progresivo e invariable para cada acto; b) Análisis de la forma personificada y la verificación de la existencia o inexistencia de antecedentes regístrales y, en su caso, preinscripción de dicha información a la base de datos ubicada en la entidad federativa; c) Calificación, en la que se autorizara en definitiva la inscripción en la base de datos mediante la firma electrónica del servidor público competente, con lo cual se generara o adicionara el folio mercantil electrónico correspondiente, y d) Emisión de una boleta de inscripción que será entregada física o electrónicamente. El reglamento del presente Capítulo desarrollara el procedimiento registral de acuerdo con las bases anteriores.

Artículo 21 bis 1.- La prelación entre derechos sobre dos o más actos que se refieran a un mismo folio mercantil electrónico, se determinara por el numero de control que otorgue el registro, cualquiera que sea la fecha de su constitución o celebraciones.

Artículo 22.- Cuando, conforme a la ley, algún acto o contrato deba inscribirse en el Registro Público de la Propiedad o en registros especiales, su inscripción en dichos registros será bastante para que surtan los efectos correspondientes del derecho mercantil, siempre y cuando en el Registro Público de Comercio se tome razón de dicha inscripción y de las modificaciones a la misma.

Artículo 23.- Las inscripciones deberán hacerse en la oficina del Registro Público de Comercio del domicilio del comerciante, pero si se trata de bienes raíces o derechos reales constituidos sobre ellos, la inscripción se hará, además, en la oficina correspondiente a la ubicación de los bienes, salvo disposición legal que establezca otro procedimiento.

Artículo 24.- Las sociedades extranjeras deberán acreditar, para su inscripción en el Registro Público de Comercio, estar constituidas conforme a las leyes de su país de origen y autorizadas para ejercer el comercio por la Secretaria, sin perjuicio de lo establecido en los tratados o convenios internacionales.

Artículo 25.- Los actos que conforme a este Código u otras leyes deban inscribirse en el Registro Público de Comercio deberán constar en: I.- Instrumentos públicos otorgados ante notario o corredor público; II.- Resoluciones y providencias judiciales o administrativas certificadas; III.- Documentos privados ratificados ante notario o corredor público, o autoridad judicial competente, según corresponda, o IV.- Los demás documentos que de conformidad con otras leyes así lo prevean.

Artículo 26.- Los documentos de procedencia extranjera que se refieran a actos inscribibles podrán constar previamente en instrumento público otorgado ante notario o corredor público, para su inscripción en el Registro Público de Comercio. Las sentencias dictadas en el extranjero solo se registraran cuando medie orden de autoridad judicial mexicana competente, y de conformidad con las disposiciones internacionales aplicables.

Artículo 27.- La falta de registro de los actos cuya inscripción sea obligatoria, hará que éstos solo produzcan efectos jurídicos entre los que lo celebren, y no podrán producir perjuicio a tercero, el cual si podrá aprovecharse de ellos en lo que le fueren favorables.

Artículo 30.- Los particulares podrán consultar las bases de datos y, en su caso, solicitar las certificaciones respectivas, previo pago de los derechos correspondientes. Las certificaciones se expedirán previa solicitud por escrito que deberá contener los datos que sean necesarios para la localización de los asientos sobre los que deba versar la certificación y, en su caso, la mención del folio mercantil electrónico correspondiente. Cuando la solicitud respectiva haga referencia a actos aún no inscritos, pero ingresados a la oficina del Registro Público de Comercio, las certificaciones se referirán a los asientos de presentación y tramite.

Artículo 30 bis.- La Secretaria podrá autorizar el acceso a la base de datos del Registro Público de Comercio a personas que así lo soliciten y cumplan con los requisitos para ello, en los términos de este Capítulo, el reglamento respectivo y los lineamientos que emita la Secretaria, sin que dicha autorización implique en ningún caso inscribir o modificar los asientos regístrales. La Secretaria certificara los medios de identificación que utilicen las personas autorizadas para firmar electrónicamente la información relacionada con el Registro Público de Comercio, así como la de los demás usuarios del mismo, y ejercer el

control de estos medios a fin de salvaguardar la confidencialidad de la información que se remita por esta vía.

Artículo 30 bis.- Cuando la autorización a que se refiere el artículo anterior se otorgue a notarios o corredores públicos, dicha autorización permitirá, además, el envío de información por medios electrónicos al Registro y la remisión que éste efectúe al fedatario público correspondiente del acuse que contenga el numero de control a que se refiere el artículo 21 bis 1 de este Código. Los notarios y corredores públicos que soliciten dicha autorización deberán otorgar una fianza a favor de la Tesorería de la Federaciones y registrarla ante la Secretaria, para garantizar los daños que pudieran ocasionar a los particulares en la operación del programa informático, por un monto mínimo equivalente a 10 000 veces el salario mínimo diario vigente en el Distrito Federal. En caso de que los notarios o corredores públicos estén obligados por la ley de la materia a garantizar el ejercicio de sus funciones, solo otorgaran la fianza a que se refiere el párrafo anterior por un monto equivalente a la diferencia entre ésta y la otorgada. Dicha autorización y su cancelación deberán publicarse en el Diario Oficial de la Federaciones.

Artículo 31.- Los registradores no podrán denegar la inscripción de los documentos mercantiles que se les presenten, salvo cuando: I. El acto o contrato que en ellos se contenga no sea de los que deben inscribirse; II. Esté en manifiesta contradicción con los contenidos de los asientos regístrales preexistentes, o III. El documento de que se trate no exprese,

o exprese sin claridad suficiente, los datos que deba contener la inscripción. Si la autoridad administrativa o judicial ordena que se registre un instrumento rechazado, la inscripción surtirá sus efectos desde que por primera vez se presento. El registrador suspenderá la inscripción de los actos a inscribir, siempre que existan defectos u omisiones que sean subsanables. En todo caso se requerirá al interesado para que en el plazo que determine el reglamento de este Capítulo las subsane, en el entendido de que, de no hacerlo, se le denegara la inscripción.

Artículo 32.- La rectificación de los asientos en la base de datos por causa de error material o de concepto, solo procede cuando exista discrepancia entre el instrumento donde conste el acto y la inscripción. Se entenderá que se comete error material cuando se escriban unas palabras por otras, se omita la expresión de alguna circunstancia o se equivoquen los nombres propios o las cantidades al copiarlas del instrumento donde conste el acto, sin cambiar por eso el sentido general de la inscripción ni el de alguno de sus conceptos. Se entenderá que se comete error de concepto cuando al expresar en la inscripción alguno de los contenidos del instrumento, se altere o varíe su sentido porque el responsable de la inscripción se hubiere formado un juicio equivocado del mismo, por una errónea calificación del contrato o acto en él consignado o por cualquiera otra circunstancia similar.

Artículo 32 bis.- Cuando se trate de errores de concepto, los asientos practicados en los folios del Registro Público de Comercio solo podrán

rectificarse con el consentimiento de todos los interesados en el asiento. A falta del consentimiento unánime de los interesados, la rectificación sólo podrá efectuarse por resolución judicial. El concepto rectificado surtirá efectos desde la fecha de su rectificación. El procedimiento para efectuar la rectificación en la base de datos lo determinara la Secretaria en los lineamientos que al efecto emitan.

Artículo 49.- Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

Bueno nos queda claro que en el registro público se llevan a cabo las inscripciones tanto de inmuebles como de actos mercantiles y que las mismas deben operar con un sistema informático acorde con la demanda del servicio llevado acabo por el Registro, ahora bien esta reforma en su afán de hacer más ágil la función tanto de notarios como de su personal como registradores, ha tratado de automatizar los servicios que ofrece, a mi parecer aún falta mucho por

hacer ya que en la realidad el Registro de instrumentos públicos es muy tardado, haciendo del funcionamiento del Registro algo automatizado, podríamos llegar a uno de los fines que buscamos al plantear este trabajo el ahorro de tiempo y dinero.

5.7 Conservación de datos.

La conservación de datos se encuentra regulada en la Norma oficial mexicana NOM-151-SCFI-2002 de prácticas comerciales, requisitos que deben observarse para la conservación de mensajes de datos; la cual fue publicada en el Diario Oficial de la Federación del 4 de junio de 2002.

El antecedente de esta Norma lo encontramos en el proyecto de la Norma Oficial mexicana NOM-151-SCFI-2002 practicas comerciales y requisitos que deben observarse para la conservación de mensajes de datos publicada en el Diario Oficial de la Federación del 16 de noviembre de 2001.

En este proyecto intervinieron empresas del sector privado instituciones del sector público e inclusive el poder judicial de la Federación, este proyecto se fundamento en el artículo 40 fracción III y XVIII de la Ley Federal sobre Metrología y Normalización en relación con el Artículo 49 del Código de Comercio.

De acuerdo a lo anterior definiremos a las Norma Oficial Mexicana", como una regulación técnica de observación obligatoria, expedida por las dependencias competentes conforme a las finalidades establecidas en el citado artículo 49 que establece reglas, especificaciones, atributos, características o prescripciones aplicables a un producto, proceso, instalación sistema, actualidad, servicio o

método de producción u operación, así como aquellas relativas o terminología simbología embalge marcado y las que se refieren a su cumplimiento o aplicación."[167]

5.7.1 NORMA OFICIAL MEXICANA NOM-151-SCFI-2002, PRACTICAS COMERCIALES

Publicado en la Primera Sección del DIARIO OFICIAL de la federación el martes 4 de junio de 2002, por el que la Secretaria de Economía establece los requisitos que deben observarse para la conservación de mensajes de datos, participando en la elaboración de la presente Norma Oficial Mexicana empresas e instituciones; tales como Acertia Networks, S.A. De C.V., La Asociación Mexicana De Estándares Para El Comercio Electrónico, A.C., La Asociación Mexicana De La Industria De Tecnologías De Información, A.C., El Banco De México, El Banco Internacional, S.A., El Banco Nacional De México, S.A., BBVA Bancomer, S.A., La Cámara Nacional De La Industria Electrónica, De Telecomunicaciones E

[167] Normas Oficiales Mexicanas tienen, como finalidad. - Establecer, las características y/o espeficaciones relacionadas con los instrumentos para medir los patrones de medida y sus métodos de mediación, verificación, calibración y trazabilidad;
- La nomenclatura, expresiones, abreviaturas, símbolos, diagramas o dibujos que deberán emplearse en el lenguaje técnico instrumental, comercial, deservicios o de comunicación.
- Las características y especificaciones que deban reunir los aparatos reales y sistemas de comunicación, así como vehículos de transporte, equipos y servicios anexos para proteger las vías generales de comunicación y la seguridad de sus usuarios.
- Los límites del uso del certificado, si se prevén como por ejemplo compra a través de Internet, acceso a bancos exclusivos de ciertos contratos, como préstamos y fianzas, ante servidores en una red local.
- Los límites del valor de las transacciones, para las averiguaciones pueden utilizarse el certificado si se establecen de esta forma se controla que con un certificado no puedan efectuarse compras por un importe superior o un valor especificado en el mismo. DIARIO OFICIAL DE LA FEDERACIÓN (Primera Sección) del Martes 4 de junio de 2002.

Informática, El Poder Judicial Federal, La Secretaria De Economía., El Servicio De Administración Tributaria, entre otros, y la que de alguna manera es un glosario de las definiciones que ya analizamos anteriormente, versando de la siguiente manera:

“. . . 3. Definiciones

4. Disposiciones generales

5. Elementos que intervienen en la conservación de mensajes de datos

6. Vigilancia

7. Apéndice normativo

8. Bibliografía

9. Concordancia con normas internacionales

Transitorio

3. Definiciones

3.1 Aceptación de autoría: A la propiedad de un algoritmo de firma digital que permite atribuir a una persona física o moral la autoría de un mensaje de datos inequívocamente.

3.2 Acto de comercio: A todo acto que la legislación vigente considera como tal.

3.3 Autenticación: Al proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros.

3.4 Archivo parcial: Al mensaje de datos representado en formato ASN.1, conforme al apéndice de la presente Norma Oficial Mexicana.

3.5 ASN.1: A la versión 1 de Abstracts Sintax Notation (Notación Abstracta de Sintaxis).

3.6 Bits: A la unidad mínima de información que puede ser procesada por una computadora.

3.7 Bytes: A la secuencia de 8 bits.

3.8 Clave pública: A la cadena de bits perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada.

3.9 Clave privada: A la cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos.

3.10 Certificado digital: Al mensaje de datos firmado electrónicamente que vincula a una entidad con una clave pública.

3.11 Código: Al Código de Comercio.

3.12 Código de error: A la clave indicativa de un suceso incorrecto.

3.13 Comerciantes: A las personas físicas o morales a los que la legislación les otorga tal carácter.

3.14 Compromiso: A cualquier acto jurídico diferente del contrato o del convenio, que genere derechos y obligaciones.

3.15 Confidencialidad: Al estado que existe cuando la información permanece controlada y es protegida de su acceso y distribución no autorizada.

3.16 Contrato: Al acuerdo de voluntades que crea o transfiere derechos y obligaciones.

3.17 Convenio: Al acuerdo de voluntades que crea, transfiere, modifica o extingue derechos y obligaciones.

3.18 Constancia del prestador de servicios de certificación: Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente Norma Oficial Mexicana.

3.19 Criptografía: Al conjunto de técnicas matemáticas para cifrar información.

3.20 Destinatario: A aquella entidad a quien va dirigido un mensaje de datos.

3.21 Emisor: A aquella entidad que genera y transmite un mensaje de datos.

3.22 Entidad: A las personas físicas o morales.

3.23 Expediente electrónico: Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente norma oficial mexicana.

3.24 Firma digital: A la firma electrónica que está vinculada al firmante de manera única, permitiendo así su identificación, creada utilizando medios que aquél pueda mantener bajo su exclusivo control, estando vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. La firma digital es una especie de firma electrónica que garantiza la autenticidad e integridad y la posibilidad de detectar cualquier cambio ulterior.

3.25 Firma electrónica: A 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 dicho firmante aprueba la información recogida en el mensaje de datos. La firma electrónica establece la relación entre los datos y la identidad del firmante.

3.26 Formato: A la secuencia claramente definida de caracteres, usada en el intercambio o generación de información.

3.27 Legislación: A las normas jurídicas generales y abstractas emanadas del Congreso de la Unión, así como la normatividad emanada del Poder Ejecutivo.

3.28 Mensaje de datos: A la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

3.29 Objetos: A las definiciones del lenguaje ASN.1

3.30 Original: A la información contenida en un mensaje de datos que se ha mantenido íntegra e inalterada desde el momento en que se generó por primera vez en su forma definitiva.

3.31 Prestador de servicios de certificación: A la entidad que presta los servicios de certificación a que se refiere la presente Norma Oficial Mexicana.

3.32 Red: Al sistema de telecomunicaciones entre computadoras.

3.33 Resumen o compendio: Al resultado de aplicarle a un mensaje de datos una función de criptografía del tipo *hash*.

3.34 Sello del prestador de servicios de certificación: Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente Norma Oficial Mexicana.

3.35 Secretaría: A la Secretaría de Economía.

4. Disposiciones generales

4.1 Los comerciantes deberán conservar los mensajes de datos de acuerdo al método que se describe en el Apéndice de la presente Norma Oficial Mexicana.

4.2 La información que se desee conservar se podrá almacenar en uno o varios archivos diferentes y/o en una o varias computadoras.

4.3 Sin perjuicio de lo que dispongan otros ordenamientos jurídicos aplicables, cuando se pretenda conservar en un medio electrónico, óptico o de cualquier otra tecnología, información derivada de un acto de comercio, que se encuentre soportada en un medio físico similar o distinto a aquellos, los comerciantes podrán optar por migrar dicha información a una forma digital y, observar para su conservación en forma digital, las disposiciones a que se refiere la presente Norma Oficial Mexicana. La migración de la información deberá ser cotejada por un tercero legalmente autorizado, que constatará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva. El tercero legalmente autorizado deberá ser una persona física o moral que cuente con la capacidad tecnológica suficiente y cumpla con los requisitos legales aplicables.

4.4 Los programas de cómputo (*software)* para la conservación de los mensajes de datos deberán dar cumplimiento a lo establecido por la presente Norma Oficial Mexicana.

5. Elementos que intervienen en la conservación de mensajes de datos

5.1 Para la emisión de la firma electrónica y/o digital, así como el prestador de servicios de certificación, deberán observar los requisitos que la normatividad aplicable señale para su operación.

5.2 La constancia emitida por el prestador de servicios de certificación deberá observar los términos establecidos en el Apéndice de la presente Norma Oficial Mexicana.

5.3 Los programas informáticos en y con los que se almacenen los mensajes de datos a los que se refiere la presente Norma Oficial Mexicana, utilizarán los formatos para mensajes de datos en los términos establecidos en el Apéndice del mismo.

6. Vigilancia

La vigilancia de la Norma Oficial Mexicana estará a cargo de la Secretaría conforme a sus atribuciones y la legislación aplicable.

7. Apéndice Normativo[168]

[168] En este Apéndice normativo se presentan los elementos necesarios para la implantación de la presente Norma Oficial Mexicana; la descripción del algoritmo de conservación de información y la definición ASN.1 de los objetos usados.
Se describe brevemente el algoritmo y se muestran dos archivos de texto que serán usados para construir los objetos ASN.1 resultantes de aplicar la presente Norma Oficial Mexicana a estos dos archivos.
Los objetos ASN.1 creados son mostrados a través de un vaciado hexadecimal de su contenido en formato BER. Se incluyen las claves de criptografía que se usaron en la

. . . **OBTENCIÓN DE LA CONSTANCIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN**

Para la obtención de la *constancia* el sistema de conservación deberá usar el protocolo de aplicación descrito en este apéndice para enviar el *expediente* al prestador de servicios de certificación, quien emitirá una *constancia* en formato ASN.1 y la regresará al sistema de conservación, haciendo uso del mismo protocolo.

El expediente opcionalmente podrá enviarse como un anexo de correo electrónico, siendo aplicables en este caso los protocolos Internet correspondientes.

También podrá usarse la transmisión vía Web siempre que el expediente se reciba como un archivo y siempre que se utilice un

---

creación de los ejemplos con el propósito de que se pueda verificar la implantación de la presente Norma Oficial Mexicana.

El contenido de los archivos, las definiciones pertenecientes al lenguaje ASN.1 y los archivos ASN.1 aparecen con el tipo Courier New. Cuando se use el nombre de un objeto ASN.1 dentro del texto, éste aparecerá en *itálicas.* Como referencia se presenta el juego de caracteres ISO 8859-1 (Latín 1).

FORMACIÓN DE ARCHIVOS PARCIALES

Para formar un *archivo parcial* se crea un mensaje en formato ASN.1 que contiene (i) el nombre del archivo del sistema de información en el que está o estuvo almacenado el contenido del archivo, (ii) el tipo del archivo, y (iii) el contenido del mismo; con el objetivo de guardar la relación lógica que existe entre estos tres elementos.

OBTENCIÓN DE LOS COMPENDIOS O RESÚMENES DIGITALES

Se calcula el compendio o resumen digital del *archivo o archivos parciales* resultado del proceso anterior, usando el algoritmo MD5.

INTEGRACIÓN DEL EXPEDIENTE ELECTRÓNICO

Para conformar un *expediente electrónico* se creará un mensaje ASN.1 que contiene **(i)** el nombre del *expediente*, que debe de coincidir con el nombre con el que se identifica en el sistema de información en donde está o estuvo almacenado, **(ii)** un índice, que contiene el nombre y el compendio de cada *archivo parcial* que integra el *expediente,* **(iii)** la identificación del operador del sistema de conservación, y **(iv)** su firma digital de acuerdo a la definición correspondiente en la presente Norma Oficial Mexicana. DIARIO OFICIAL DE LA FEDERACIÓN, op cit.

directorio protegido por nombre de usuario y contraseña. Para ello, la forma en que lo envíe deberá ser como la siguiente:

<form action="url del programa generador de constancias " method="post"

enctype="multipart/form-data">

Expediente: <input type="file" name="expediente">

<input type="submit" value="Obtener Constancia">

</form>

La constancia deberá regresar al cliente como un archivo de tipo mime application/octet-stream1.

El prestador de servicios de certificación podrá recibir, si así lo acuerda con sus clientes, medios físicos conteniendo los archivos correspondientes a los expedientes.

FORMACIÓN DE LA CONSTANCIA

El prestador de servicios de certificación formará una *constancia* en formato ASN.1 que contendrá **(i)** el nombre del archivo en donde está almacenada la *constancia*, **(ii)** el *expediente* enviado por el sistema de conservación, **(iii)** fecha y hora del momento en que se crea la *constancia*, **(iv)** la identificación del prestador de servicios de certificación y **(v)** su firma digital de acuerdo a la definición correspondiente de esta Norma Oficial Mexicana.

MÉTODO DE VERIFICACIÓN DE AUTENTICIDAD

La verificación de la autenticidad de una *constancia* se realizará por medio del uso de un sistema de verificación que lleve a cabo los pasos siguientes:

i) verificar la firma digital del prestador de servicios de certificación en la *constancia*;

ii) verificar la firma digital del operador del sistema de conservación en el *expediente* contenido en la *constancia*, y

iii) recalcular el compendio de él o los *archivos parciales* y verificar que coincidan con los compendios asentados en el *expediente*.

Claves privadas usadas para firmar

Con el propósito de poder verificar los objetos ASN.1 definidos en este documento se incluyen las claves privadas que fueron usadas para generar las firmas de los documentos mencionados. Durante el proceso de generación de claves no se generó la clave pública y ya se ha perdido la información de generación de dichas claves. "[169]

5.8 Efectos y alcance legal de la firma electrónica.

Los efectos tienen que vencer un criterio denominado equivalente, funcional y tiene su origen en la búsqueda de elementos que convertían a los documentos con un soporte papel como algo indiscutible es decir este criterio tiene como objetivo buscar la eliminación, en todos los textos legales, todos aquellos preceptos que encubran al soporte en papel, como el único medio de

[169] Ídem.

manifestación de la voluntad, así como el requisito de la firma manuscrita para conferirle un nexo vincula torio, ya que todo este tipo de preceptos limitaban el desarrollo del comercio electrónico.[170]

Así es sé analizaron todos los elementos que hacen al papel el medio idóneo para dar forma a los actos jurídicos con el fin de que una vez desentrañados comprobar la posibilidad existente de ser sustituidos por métodos electrónicos que en ningún momento menoscaben, las características y ventajas, que el papel confiere tratando entonces de encontrarle un equivalente para poder atribuirle el mismo reconocimiento legal.

Al concurrir en un acto jurídico, la legislación. Establece el alcance de la intervención de las personas según sea la naturaleza del documento donde aparece la firma, así pues se puede signar en las constancias para dar fé pública, autenticarla o ratificarlos. Tal es el caso de los peritos, testigos, notarios públicos, directores de Registro Público de la Propiedad, jueces del registro civil y en general todo funcionario que por suposición legal tiene que dar fé o autentificar un acto lo cual producirá diversos efectos jurídicos.

Así entonces para determinar los efectos jurídicos de una firma electrónica recordemos que existe tanto la firma electrónica avanzada como la simple; en ambas, para que produzcan efectos deberán estar basados en un certificado reconocido y deberán haber sido producidos por un dispositivo seguro de creación de firma en tal caso, respecto a los datos consignados electrónica, tendrá el mismo valor jurídico, que la firma manuscrita, en relación con los datos,

[170] MARTÍNEZ NADAL, Apol-Lonia op cit, p 331.

consignados en papel y se puede admitir en juicio y se valorara de acuerdo a los criterios de apreciación que por lo tanto no le serán negados efectos jurídicos ni serán excluidos como pruebas en juicio por el simple hecho de presentarse en forma electrónica. [171]

5.9 Propuesta, iniciativas y necesidad de legislar

Más que proponer el uso de la firma digital; me parece que debe de convertirse en una necesidad evidente y real, para el sistema jurídico y económico de nuestro país; ya que el buscar regular de una manera adecuada, todo lo que implica la contracción electrónica, siempre ira encaminada al fortalecimiento del comercio y contratación vía red.

Hay que distraer que existe un buen ambiente en varios sectores de la sociedad es decir entre los involucrados, ya que se ha tratado dotar de mecanismos técnicos y legales, para hacer seguro y eficiente el uso de la tecnología en la contratación electrónica.

Como hemos mencionado dentro del proceso de contratación electrónica, por medio de una firma digital, existen elementos esenciales en los que consta la integridad y la autenticidad de los datos e informes emitidos (por medio de la criptografía), en donde el punto esencial es el de la identidad de la firma del remitente y como consecuencia de ello la seguridad, que debe tener el destinatario de que la persona con quién contrata, es realmente ella, así como que su firma pertenece efectivamente al mismo. Esta información podría ser suministrada por el

[171] Ídem.

propio firmante mediante pruebas que satisfagan al destinatario, pero también por otros medios consistentes en recibir esa confirma, por medio de un tercero, a través de una persona o instituto, que tenga la mutua confianza de ambas partes y esos terceros, son denominados, como prestatarios de servicios de certificación, que podría ser una entidad pública, por ejemplo una secretaria o una comisión especial y también esas entidades podrían pertenecer a la iniciativa privada por ejemplo: los notarios públicos, fomentando la creación de organismo con alta especialización en tecnología, así como nuevas fuentes de empleo.

Es importante señalar la necesidad, que se tiene de regular, todo el actuar de los hombres en sociedad, para una mayor convivencia y más ahora que los medios como el correo electrónico o el intercambio electrónico de datos han difundido su uso con gran rapidez en las operaciones, comerciales tanto nacionales como internacionales. Sabemos que la actividad comercial es vital, para la vida de México, y por lo tanto es necesaria su constante actualización, por lo que el aparto legislativo debe enfocar y crear un marco jurídico, que permita la integración y desarrollo del comercio y la contratación vía electrónica, o sea de una realidad a la normatividad.

Dicho marco jurídicos sugiero podría empezar, por regular las transacciones exclusivamente llevadas a cabo por mensajes electrónicos enviados por las redes de comunicación, así que al definir, de forma jurídica los términos, mensaje de datos o documento electrónico y definir a las partes que intervienen en dicho intercambio electrónico.

La regulación de las firmas y certificados electrónicos adolecen de una normativa clara debido a la diversidad legislativa que existe también del gran

número de posibles países, que pueden participar en los intercambios comerciales on-line, por eso recomiendan la intervención de un auditor externo en los procesos de validación, ya sea un notario, un secretario judicial o un funcionario administrativo en una labor que me parece tendrá que certificar su validez.

Una ley sobre firma electrónica permitirá la puesta en marcha de esta fórmula de contratación on-line de la que hablábamos. También como medio estándar de seguridad en Internet, certificara y garantizara la identidad de las partes en las transacciones electrónicas, hará confidenciales los datos y dará mayor seguridad a la red, así los contratos firmas o registros electrónicos serán tan validos como los firmados con tinta y en papel.

Los aspectos que me parece que debería de contemplar la legislación mexicana, lo cual permitirá fomentar el uso de las firmas digitales son:

- La ley debe de ser lo más general posible para permitir, su uso en distintos ámbitos en que el sistema de firma digital tiene cabida por ejemplo privacidad, seguridad, en el comercio electrónico pruebas judiciales etc.

- Equiparación de la firma digital a la firma ológrafa.

- Precisar los requisitos que deberá contener el sistema usado para firmar electrónicamente un documento.

CONCLUSIONES

El presente trabajo nos permitirá conocer más lo que significa la firma digital, su historia y su utilidad para ser empleada en la red como un acontecimiento muy reciente dado que esta cambiando drásticamente, en el ámbito mundial la forma de hacer negocios.

Ya desde los primeros orígenes del hombre este ya ideaba la forma de comunicarse con las demás personas, la manera de lógralo es a través de la escritura o signos dentro de los cuales se encuentra la firma, si bien es cierto que en su nacimiento no era tratada como un requisito sin el cual, con el pasar de los años es como el hombre comienza a firmar documentos y por lo tanto a otorgarles validez jurídica.

En nuestro país igualmente que en países de Latinoamérica, en los primeros años al nacimiento de la firma, ya se consideraba a la firma como un requisito sin el que un documento no sería valido, para lo cual los legisladores fueron dando los lineamientos para el uso de la firma autógrafa, para poder llegar al uso de la tecnología y firmar digitalmente.

Debemos reconocer que organismos internacionales se han preocupado por hacer uso de sistemas electrónicos sofisticados para firmar y autenticar documentos, tal es el caso de leyes modelo como la de la UNCITRAL o la de la Comunidad Europea, las cuales son unas de las primeras en nacer a la vida jurídica, estas leyes modelo sobre firma electrónica sirvieron de base a México, el cual en afán de dar el mismo trato a la firma electrónica que a la firma autógrafa, se baso en ellas para dar cabida a que cada vez se haga más amplio el uso de la

tecnología y por lo tanto al uso, implementación y regulación de la firma electrónica.

El marco legal en que se basa la firma digital es muy variado pero a la vez poco mencionado, es decir ya desde la Constitución Política de México ya se hablaba de documentos firmados a pesar de esto se carecía de una legislación o simplemente de un solo artículo que tratara a la firma digital, no fue hasta las reformas de 2000 que ya se comenzó a mencionar a la firma electrónica, esta reforma fue importantísima dado que en nuestro país aún no se contaba con algo expreso acerca de la firma, y más aún por que abarca materias importantes como el civil, mercantil, procesal, fiscal y atención al consumidor, campos que no pueden ir quedando rezagados en cuanto a reformas se refiere.

El trato que se le da a la firma en general es trascendental dadas las circunstancias por las que atraviesa las nuevas formas de contracción, para que la forma electrónica nazca a la vida jurídica esta debe ser considerada primeramente y de suma importancia como una forma de exteriorización y materialización de la voluntad interviniendo por lo tanto el consentimiento elemento importante en la generación de firma electrónica y ológrafa.

La criptografía es una de las ciencias que estudia la manera en firmar documentos, es decir por medio de esta se pueden “ocultar” los mensajes de datos enviados por red, esta es una de las más confiables en su uso, y uno de los caminos que podemos seguir para obtener seguridad jurídica, principio buscado por usuarios de la red poniendo de manifiesto la necesidad de que existan terceras partes de confianza como los fedatarios públicos.

La Ley sobre firma electrónica que se propone permitirá en nuestro país poner en marcha la contratación on line, ya que hoy día una de las causas por las que no ha sido aprovechado el WWW mediante la firma digital por empresas mexicanas, para realizar negocios internacionales por este medio es la falta de una legislación para la firma digital.

El ejercicio de la fe pública del notario es de alta importancia saber que la legislación notarial considera como requisito la firma los documentos pasados ante la fe del notario, con lo cual este da fe y autentifica firmándolo y sellándolo entre otros formalismos como el de conservar el documento identificación de las partes, por mencionar algunos.

Ahora bien lo anterior también es posible lógralo por medios electrónicos y sofisticados de los cuales el notario puede allegarse, y con lo cual se trata de equiparar a la firma electrónica como la firma autógrafa, es decir es más fácil de lo que se puede leer, así que el fedatario actúa como una tercera parte de confianza, dando fe igualmente por medios digitales.

El notario será una especie de medio estándar de seguridad en la red, certificara y garantizara la identidad de las partes en transacciones electrónicas, hará confidenciales los datos que le sean proporcionados y dará más seguridad a la red, así a los contratos, firmas o registros electrónicos serán tan validos como los firmados en papel

Debemos tener en cuenta los parámetros de la firma electrónica en relación con el tipo de acto en particular y las consecuencias jurídicas de dicho acto, pues podría aplicarse a casi cualquier materia ya sea civil, mercantil, fiscal etcétera.

En nuestro derecho rige el principio consensualita para la contratación, este principio no es absoluto, admite que ciertos actos para ser validos deben de constar en un documento escrito y o firmado de manera ológrafa, situación me parece debe de irse modificando de manera gradual hasta hacerlo la forma más común para contratar y obligarse, todo esto plasmado a través de un protocolo electrónico que ahorraría gran parte de tiempo y de recursos materiales, para el notario.

La entidad que debe desempeñar la función de certificación en nuestro país considero que podrían ser corporaciones de tipo público y privado, autorizadas, supervisadas, sancionadas y canceladas para operar por la Secretaria de Economía, así que el papel que jugaría un notario en la implantación de un modelo de firma electrónica en nuestro país, y actuando con cierta autonomía, lo que generaría cierta competencia con relación a la calidad, seguridad y confiabilidad de sus servicios. Así que la Secretaría de Economía seria la encargada de la conservación de datos y la firma electrónica a cargo de notarios o corredores públicos.

Aunado a lo anterior la modernización de los registros y del notariado nos han llevado a que se establezcan reglas para el mejor funcionamiento del Registro Público de la Propiedad y del Archivo General de Notarias, importante por el grado de interacción el notario público, dado que gran parte de la historia de escrituras pasadas ante su fe se encuentran en estos dos auxiliares en la función que este fedatario lleva acabo.

BIBLIOGRAFÍA

ACOSTA ROMERO, Miguel, *Derecho Bancario, panorama del sistema financiero mexicano*, 4ª edición, Editorial Porrua, México 1991.

AHRENS, Enrique, *Historia del Derecho*, Editorial De Palma, Argentina, 1945.

ALBA H, Carlos, *Estudio comparado entre derecho azteca y derecho positivo mexicano*, Editorial Ediciones Especiales del Instituto Indigenista Interamericano, México, 1949.

ÁLVAREZ CIENFUEGOS, José Maria, *Instituciones del mercado financiero (contratos bancarios): Nuevas formas de contratación: banca electrónica y telefonía*, Volumen I Fuentes protección de consumidores, responsabilidad y nuevos sistemas de contratación, SOPEC Editorial S.A. Grupo Banco Santander Central Hispano, España 1999.

APRENDA COMPUTADORAS E INTERNET VISUALMENTE, Editorial Reader's Digest S.A. de C.V., México 1999.

ARRAZOLA, Lorenzo, *Enciclopedia Española de derecho y Administración España y las Indias*, Tomo XI, Editorial Tipográfica General de D. Antonio Rius y Rossell, España,1999.

ASCARELLI, Tullio, *Derecho Mercantil Mexicano*, (DE J. TENA Felipe), 18ª edición, Editorial Porrua, México, 1999.

BAÑUELOS SÁNCHEZ, Froilán, *Derecho notarial*, 3ª edición, Editorial Cárdenas Editor y Distribuidor, México 1994.

BERNI Y CATALA, Joseph D. Dr., *Apuntamientos sobre las Leyes de Partidas al tenor de leyes recopiladas, autos acordados, autores españoles y prácticas modernas*, Editorial Imprenta de Benito Monfort, España, 1759.

BORJA SORIANO, Manuel, *Teoría General de las obligaciones*, Editorial Porrua, México, 1998.

CIENFUEGOS SUÁREZ, Juan, *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Editorial España, España, 1998.

COUTURE, Eduardo Juan, *Vocabulario Jurídico*, Editorial Depalma, Argentina, 1998.

DE PRADA, José Maria, *La forma de los actos jurídicos privados y la seguridad jurídica*., Consejo Nacional del Notariado, Universidad Internacional Menéndez Pelayo, Impresión en México, Madrid 1990.

FERNÁNDEZ MACIA, Enrique, *La protección internacional de los programas de ordenador*, Editorial Comares, España, 1998.

FLORIS MARGADANT, Guillermo, *El derecho privado romano como introducción a la cultura jurídica contemporánea*, decimoquinta edición, Editorial Esfinge, México, 1988.

FLORIS MARGADANT, Guillermo, *El derecho privado romano*, Editorial Esfinge, México, 1960.

FLORIS MARGADANT, Guillermo, *Panorama de la Historia Universal del Derecho*, 1a Reimpresión, Editorial Porrua, México, 2002.

FUSTER SABATER, Amparo, *Técnicas criptográficas de protección de datos*, 2ª edición, Editorial Alfaomega Ra-Ma, España, 2001.

GAETE GONZÁLEZ, Eugenio Alberto, *Instrumento Público Electrónico*, 2ª Edición, Editorial Bosch S.A., España 2002.

GÓMEZ-MARTINHO FAERNA, Augusto, *La función del notario en la Unión Europea: un estudio comparativo,* Editorial Junta de Decanos de los Colegios Notariales de España, España, 1997.

GRACIA DOMÍNGUEZ, Miguel Ángel. *Derecho Penal Fiscal, Las infracciones y multas fiscales*, Editorial Porrua, México, 1994.

GUTIÉRREZ FERNÁNDEZ, Benito, *Código de estudios fundamentales de Derecho Civil Español*, Tomo II, Titulo IV, Libro II precedentes patrios fuero juzgo, Editorial Librería de Sánchez, España, 1999

LIMA DE LA LUZ, Maria, *Delitos electrónicos en criminalía*, Academia Mexicana de ciencias penales, Editorial Porrua, México, No 1-6 Año L. Enero –Junio 1984.

LLANEZA GONZÁLEZ, Paloma, *Internet y comunicaciones digitales, Régimen legal de las tecnologías de la información y la comunicación,* Editorial Bosch, España 2000.

LOS CÓDIGOS ESPAÑOLES CONCORDADOS Y ANOTADOS, Editorial Imprenta La Publicidad, España, 1850.

MANTILLA MOLINA, Roberto, *Derecho Mercantil*, 29ª Edición, Editorial Porrua, México 2000.

MARTÍNEZ NADAL, Apol-Lonia, *Comercio Electrónico, Firma Digital y Autoridades de Certificación*, 3ª Edición, Editorial Civitas, España, 2001.

MARTÍNEZ NADAL APOL-LONIA, *Ley de Firma Electrónica*, 2a edición, Editorial Civitas, serie civitas monografías, España 2001.

MATEOS ALARCÓN, Manuel D, *La Evolución del Derecho Civil Mexicano, desde la Independencia hasta nuestros días*, Editorial Vda. de F Díaz de León, México, 1995.

MIRANDA, José, *Historia de México,* 12ª Edición, Editorial Porrua, México, 1983.

MORENO MARTÍN, Arturo, *Diccionario de Informática y telecomunicaciones*, Editorial Ariel, España 2001.

NANDO LEFORT, Víctor, *Diccionario Terminológico de Ciencias Forenses*, Editorial Trillas, México 1998.

NAVA GARCÉS, Alberto Enrique, *Análisis de los delitos informáticos*, Primera Edición, Editorial Porrua, México 2005.

ORTOLAN, José Luis, *Explicación histórica de las Instituciones del Emperador Justiniano* traducción (PÉREZ DE ANAYA Francisco), Editorial Hijos de Leocadio López, España, 1912.

PERALES SANZ, José Luis, *La seguridad jurídica en las transacciones electrónicas*; seminario organizado por el consejo general del notariado en la UIMP, Coedición Civitas Ediciones, España, 2002.

PÉREZ FERNÁNDEZ DEL CASTILLO, Bernardo, *Apuntes para la historia del notariado en México*, Asociación nacional del notariado mexicano, México, 1979.

PÉREZ FERNÁNDEZ DEL CASTILLO, Bernardo, *Deontología Jurídica, Ética del Abogado,* Editorial Porrua, México 1997.

PÉREZ FONTAINE, Rodolfo, *La tecnología digital*, Editorial Dykinson, México, 2000.

PÉREZ NIETO CASTRO, Leonel, *Derecho Internacional Privado*, Editorial Oxford University Press, Séptima edición, México, 2002.

PETIT, Eugene, *Tratado elemental de Derecho Romano*, Editorial Cárdenas Editor y Distribuidor, México, 1989.

PIÑA CHAN, Román, *Historia Arqueológica y Arte Prehispánico*, 1ª reimpresión, Fondo de Cultura Económica, México, 1975.

RABASA O. Emilio y CABALLERO Gloria, *Mexicano esta es tu Constitución*, undécima edición LVI Legislatura, Cámara de Diputados del H Congreso de la Unión, Grupo Editorial Porrua, México 1997.

RAMOS ITURBIDE, Bernardino, *Dictamen sobre la iniciativa de Decreto por el que se propone adicionar diversos artículos a la Ley del Notariado para el Distrito Federal,* México D.F. 20 de marzo de 2003.

REYES KRAFFT, Alfredo Alejandro, *Firma Electrónica y Entidades de Certificación*, 1ª Edición, Editorial Porrua México 2003.

ROMERO, José Luís, *La edad Media*, Editorial FCE, México, 1994.

TÉLLEZ VALDEZ, Julio, *Derecho Informático,* Segunda Edición, Editorial Mc Graw Hill, México 1996.

TOMAS Y VALIENTE, Francisco, *El orden Jurídico Medieval*, Editorial Marcial Pons Ediciones Jurídicas y Sociales S.A., España, 1996.

TORRES BALTAZAR, Edgar, *Decreto por el que se adicionan diversos artículos a la ley de notariado para el Distrito Federal*, Diputado, Asamblea legislativa del Distrito Federal, II Legislatura.

TUSON, Jesús, *La escritura una introducción a la cultura alfabética*, Ediciones Octaedro S.L. España, 1997.

VILLALPANDO MORALES, Carlos, *Transacciones electrónicas*, Editorial Destino, Argentina, 1999.

VIVIANA SARRA Andrea, *Comercio Electrónico y Derecho*, Editorial Astrea, Argentina, 2000.

ZORITA DE, Alonso, *Leyes y ordenanzas reales de las Indias*, Editorial Porrua, México, 1985.

ZORITA DE, Alonso, *Los señores de la Nueva España*, Editorial Imprenta Universitaria, México, 1942.

LEGISLACIÓN

CÓDIGO CIVIL PARA EL DISTRITO FEDERAL, Agenda Civil del Distrito Federal, Ediciones Fiscales ISEF, cuarta edición, México 2003.

CÓDIGO DE PROCEDIMIENTOS CIVILES PARA EL DISTRITO FEDERAL, Agenda Civil del Distrito Federal, Ediciones Fiscales ISEF, cuarta edición, México 2003.

CÓDIGO CIVIL ARGENTINO, ANOTADO Y CONCORDADO, Editorial Claridad, Argentina, 1999.

CÓDIGO CIVIL ESPAÑOL, 2a Edición, Colección de Textos Jurídicos, Bosch Casa Editorial, España 1989.

PUBLICACIONES

DIARIO OFICIAL DE LA FEDERACIÓN, *Reformas y adiciones diversas disposiciones del Código Civil para el Distrito Federal en materia común y para toda la República en materia federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor,* Publicado el día 29 mayo de 2000.

DIARIO OFICIAL DE LA FEDERACIÓN, Servicio de Administración Tributaria. Secretaría de Economía *Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en materia de Firma Electrónica* Publicado el 29 de agosto de 2003. [En línea]. Disponible: http://www.sat.gob.mx/

DIARIO OFICIAL DE LA FEDERACIÓN de 16 de junio de 2003

DIARIO OFICIAL DE LA FEDERACIÓN (Primera Sección) del Martes 4 de junio de 2002.

DIARIO OFICIAL DE LA FEDERACIÓN, *Decreto de promulgación del Tratado de Libre Comercio de América del Norte*, publicado en el Tomo CDLXXXII, No. 14, 20 de Diciembre de 1993.

DICCIONARIOS Y ENCICLOPEDIAS

DICCIONARIO DE LA REAL ACADEMIA DE LA LENGUA ESPAÑOLA, Vigésima Edición, Tomo I, Editorial Espasa Calpe, España, 1990.

ENCICLOPEDIA JURÍDICA ESPAÑOLA T. XVI, Editorial Francisco Seix Editor, España 1910.

ENCICLOPEDIA JURÍDICA OMEBA, Tomo XIII, Editorial Bibliográfica Fami-Gora, Argentina, 1974.

GRAN ENCICLOPEDIA LAROUSSE, Tomo IV, Editorial Planeta, S.A., México, 1972.

INTERNET

Anguiano & Asociados, Abogados, Departamento de Comercio Electrónico, Requisitos de las Autoridades de Certificación según el Grupo de Trabajo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, [En Línea]. Disponible: http://www.arrakis.es/~anguiano/artautcert.html

Cámara Nacional de Comercio, Servicios y Turismo de Chile, Entidad de Certificación electrónica, Prácticas de Certificación Digital (PCD) CNC-ONCE [En línea]. Disponible: http://www.cnc-once.cl/prac_cert.htm

Centro de Investigaciones en Information Technology. Firma digital Proyecto Cybernotario 20 marzo 2002 [En línea]. Disponible: http://www.it-cenit.org.ar/

Cibernauta.com Microsoft y el Consejo General de Notariado alcanzan un acuerdo para impulsar la firma electrónica 20/12/2005, [En línea]. Disponible: http://www.elcorreodigital.com

Código de Procedimiento Civil Colombiano. Senado de la República de Colombia, Información legislativa Leyes desde 1992 - Vigencia Expresa y Sentencias de Constitucionalidad, 9 de marzo de 2006. [En línea]. Disponible: http://www.secretariasenado.gov.co/

CÓDIGO FISCAL DE LA FEDERACIÓN Instituto de Investigaciones Jurídicas, Información Jurídica, Legislación Federal Texto vigente al 30 de noviembre de 2005, [En línea]. Disponible: http://info4.juridicas.unam.mx

CUERVO ÁLVAREZ, José. La firma digital y entidades de certificación 1998-2002 [En línea]. Disponible: http://www.informatica-juridica.com/

DEVOTO, Mauricio y M. LYNCH, Horacio, Banca, Comercio, Moneda Electrónica y Firma Digital, Proyecto Cybernotario, Publicaciones CENIT, [En línea]. Disponible: http://www.it-cenit.org.ar/Publicac/BancaMD/BanCom5

DÍAZ GARCÍA, Alexander, REDI Revista Electrónica de Derecho Informático, Los Documentos Electrónicos y sus Efectos Legales en Colombia, Numero 34, Mayo 2001 [En línea]. Disponible: http://premium.vlex.com/doctrina/REDI

El Rincón de Quevedo. Criptografía. [En línea]. Disponible: http://www.rinconquevedo.iespana.es/rinconquevedo/Criptografia/rsa2000.htm

FERNÁNDEZ DELPECH, Horacio, Trabajo preparado por un grupo de alumnos de la Cátedra Marco Legal a cargo del Dr. Horacio Fernández Delpech, del Master año 2004 en Dirección de Empresas dictado por USAL (Argentina) - Universidad

de Deusto (España) Alumnos autores: Carlos Fernando Barberán, et. al, Firma Digital [En línea]. Disponible: http://www.hfernandezdelpech.com.ar/

Gobierno Bolivariano de Venezuela, Ministerio de Ciencia y Tecnología, Centro Nacional de Tecnologías de la Información, Directorio de Gobierno Electrónico Venezuela, Decreto 825, 10 mayo 2000. [En línea] Disponible: http://www.gobiernoenlinea.gob.ve/directorioestado/decreto_825.html

Hispasec Sistemas, Seguridad y tecnologías de la Información, Inseguridad en la firma electrónica 05/03/2000 [En línea]. Disponible: http://www.hispasec.com/

Iniciativas presentadas previas al Decreto de Reforma de 2000 [En línea]. Disponible: http://www.amece.com.mx

ITEnLinea Administración Estratégica del Recurso Informático. Importancia de la firma digital Por: Wilson Barón, Director de Operaciones para la Región Andina de Afina 16 septiembre 2005 [En línea]. Disponible: http://www.itenlinea.com/

Leggio, Contenidos y Aplicaciones Informáticas, S.L. Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico 11/07/2002. [En línea]. Disponible: http://www.juridicas.com/base_datos/Admin/l34-2002.html

LUCENA, Manuel, Kriptopolis, privacidad, identidad, seguridad, Mensajería Instantánea y segura, 27 mayo 2003 [En línea]. Disponible: http://www.kriptopolis.org/node/1185

MARTÍNEZ CASTAÑO, Juan Antonio, Voto Electrónico y Software Libre, 2000 [En Línea]Disponible:http://oasis.dit.upm.es/~jantonio/documentos/voto-electronico/article.html

Ministerio de Industria, Turismo y Comercio, Real Decreto-Ley 14/1999 de 17 de septiembre, sobre firma electrónica, (derogada por Ley 59/2003, de firma electrónica). [En línea]. Disponible: http://wwwsetsi.mcyt.es/legisla/internet/rdley14_99.htm

MORENO, Luciano, *Manual de criptografía*, Departamento de diseño web BJS Software. [En línea]. Disponible: http://www.htm/web.net/seguridad/cripto/cripto_1.htm/

RAMOS SUÁREZ, Fernando, Como aplicar la nueva normativa sobre firma electrónica, Noticias jurídicas del 25 de febrero de 2000, [En línea]. Disponible: http://www.noticiasjurídicas.com/

REYES KRAFFT, Alfredo Alejandro. La firma electrónica [En línea]. Disponible: http://www.razonypalabra.org.mx

Seguri Data, SeguriDoc, Integridad, autenticidad, no repudio de origen y confidencialidad para sus archivos, [En línea]. Disponible: http://www.seguridata.com/Brochure SeguriDoc.pdf

Subsecretaria de la Gestión Publica, Jefatura de Gabinete de Ministros. República de Argentina Infraestructura de Firma Digital de la República Argentina 5 enero de 2006 [En línea]. Disponible: http://www.pki.gov.ar/

Wikipedia, Enciclopedia Libre, Criptografía, 28 marzo 2006, [En línea]. Disponible: http://es.wikipedia.org/wiki/Criptograf%C3%ADa