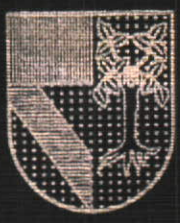

UNIVERSIDAD PANAMERICANA
CAMPUS GUADALAJARA

KARINA ALCÁZAR LÓPEZ

LA RATIFICACIÓN DE LA FIRMA DIGITAL ANTE NOTARIO PÚBLICO

Tesis presentada para optar por el título de Licenciado en Derecho con Reconocimiento de Validez Oficial de Estudios de la SECRETARÍA DE EDUCACIÓN PÚBLICA, según acuerdo número 86809 con fecha 13-VIII-86.

Zapopan, Jal., Febrero de 2005.

UNIVERSIDAD PANAMERICANA
CAMPUS GUADALAJARA

KARINA ALCÁZAR LÓPEZ

LA RATIFICACIÓN DE LA FIRMA DIGITAL ANTE NOTARIO PÚBLICO

Tesis presentada para optar por el título de Licenciado en Derecho con Reconocimiento de Validez Oficial de Estudios de la SECRETARÍA DE EDUCACIÓN PÚBLICA, según acuerdo número 86809 con fecha 13-VIII-86.

Zapopan, Jal., Febrero de 2005.

131h.; 24cm. + 1 disco flexible

500 Publicado también en forma electrónica en formato PDF para la comunidad universitaria de la UP

502. Tesis (Licenciatura) - Universidad Panamericana Campus Guadalajara, 2005

504. Bibliografía: h. 129-131

1. Tesis y disertaciones académicas - Universidad Panamericana Campus Guadalajara, 2005
2. Contratos mal
3. Derecho notarial

346.02 ALC 2005

UNIVERSIDAD PANAMERICANA

CAMPUS GUADALAJARA

ESCUELA DE DERECHO

DICTAMEN DEL TRABAJO DE TITULACIÓN

C. KARINA ALCAZAR LÓPEZ
P r e s e n t e

En mi calidad de Presidente de la Comisión de Exámenes Profesionales y después de haber analizado el trabajo de titulación en la opción TESIS titulado: **"LA RATIFICACIÓN DE LA FIRMA DIGITAL ANTE NOTARIO PÚBLICO"** presentado por usted, le manifiesto que reúne los requisitos a que obligan los reglamentos para ser presentado ante el H. Jurado del Examen Profesional, por lo que deberá entregar ocho ejemplares como parte de su expediente al solicitar el examen.

Atentamente

EL PRESIDENTE DE LA COMISIÓN

LIC. ALBERTO JOSÉ ALARCÓN MENCHACA

TORRES
& ENRIGUE
ABOGADOS

Carlos Enrigue Zuloaga

Guadalajara, Jal., 06 de Febrero mca 2004

UNIVERSIDAD PANAMERICANA
CAMPUS GUADAJARA
COMITE DE EXAMENES PROFESIONALES
PRESENTE

En mi calidad de Director de Tesis, por medio de la presente hago de su conocimiento, que la señorita Karina Alcázar López término su proyecto de tesis titulado "La Ratificacion de la Firma Digital ante Notario Público".

Por lo anterior, otorgo al trabajo de tesis con antelación referido, mi voto de aprobación y les solicito que por favor sigan los pasos necesarios para la conclusión de dicho trabajo.

Agradeciendo de antemano la atención a la presente, quedo como su seguro y atento servidor.

ATENTAMENTE

LIC. CARLOS ENRIQUE ZULOAGA

v. Libertad 1828 Sector Juarez Tels: 825-2524 825-2529 825-2534 825-2633 826-0408 826-0367 826-0315 826-0182 Fax (3) 825-1719 Guadalajara, Jalisco Mexico C.P.

A Dios por ser tan benevolente conmigo.

En forma destacada mis papas por su paciencia y apoyo,
ya que sin ellos no lo hubiera logrado.

A mis amigos que siempre me han asistido
en los momentos más difíciles.

A los que me han criticado y me han ignorado incluso
a los que no creyeron en mí a ellos,
les voy a demostrar lo lejos que voy a llegar
por difícil que sea el camino.

A todos lo que me apoyaron y siempre están conmigo
a ellos gracias.

A mí gran amigo y amor de mi vida gracias
por tu infinita paciencia y por ser mi inspiración
a ser cada día mejor.

ÍNDICE

CAPÍTULO IV.- FIRMA ELECTRÓNICA, FIRMA DIGITAL Y CERTIFICADOS DIGITALES

CAPÍTULO V.- PROCESOS DE LAS FIRMAS DIGITALES

INTRODUCCIÓN

Iniciar una tesis es siempre un motivo de preocupación, que produce que uno dude incluso de los conocimientos que ya tiene; por otro lado produce una serie de intentos fallidos, dudas de entre hacer una investigación que no sabemos si llegará a un fin o en su lugar tratar de justificar una idea que ya se encuentra preconcebida.

He decidido avanzar entre ambos intentos y justificar, no mi idea preconcebida sino la realidad en la que se muestra que la expresión del consentimiento en el mundo ha rebasado las consideraciones de las legislaciones formales.

En nuestro derecho se utiliza un concepto inexacto del consentimiento, se supone siempre la conducta bis a bis del oferente y del aceptante, estableciendo la legislación que sólo este último instante en el que se da la aceptación es lisa y llana forma el consentimiento.

Es por eso que he decidido intentar como tesis profesional un análisis de la firma electrónica como nueva fórmula de expresión de voluntad, esperando que estas consideraciones rebasen su primigenia necesidad que es la de ser un medio para obtener el título profesional y pueda continuar posteriormente dicho estudio.

Todos conocemos la firma manuscrita como un requisito para demostrar el consentimiento en un contrato, transacción, acuerdo, etcétera. La firma es utilizada prácticamente todos los días y en todas las actividades, incluso cotidianas. La firma es entonces, el punto determinante para la aceptación de cualquier acuerdo, pero, ¿qué pasa si esta firma evoluciona? ¿Será igualmente aceptada en las actividades cotidianas? ¿Tendrá el mismo valor que una firma manuscrita?

En la actualidad, por medio de la tecnología, el consentimiento y su manifestación han expandido sus fronteras hasta el punto de hacerlas prácticamente inexistentes; un punto muy importante para esta expansión ha sido la aparición y aceptación de la internet. Por este medio ya se realizan millones de transacciones, compras, aceptaciones, acuerdos, etcétera. La variedad y cantidad de operaciones es impresionante. Sin embargo, hay muchas cuestiones por resolver: ¿Dónde queda plasmada nuestra firma? Si es reconocida normalmente como la prueba del consentimiento, ¿es válido nuestro contrato por comprar algo por internet? ¿Qué pasa si alguien nos defrauda? ¿A quién recurrimos?

Estas y más preguntas nos embargan al realizar cualquier transacción por internet. La mencionada expansión ha sido tan rápida que no se han revisado debidamente las implicaciones de aquélla y mucho menos en cada uno de los países o regiones del mundo.

En muchos países se está trabajando hoy en la legislación de la firma electrónica a fin de regular las operaciones jurídicas o legales en internet, y en nuestro caso nuestro interés se centra en México, en cómo implantará dicha regulación, así como el papel del notario y de otros fedatarios ante la firma electrónica. Este trabajo está destinado a explicar estos puntos, junto con un análisis de la firma electrónica, la criptografía (que tiene un papel esencial en aquélla), los certificados digitales, los prestadores de servicios, etcétera.

Explicaré en este mismo trabajo el principio de la Infraestructura de Claves Públicas, conocida como PKI, cómo se utiliza, qué funciones tiene, y la capacitación que requiere el personal que hará uso de este sistema.

Me basaré en las legislaciones de otros países a fin de comparar nuestro desarrollo con el de ellos, y haré énfasis en España, pues lo considero un país muy rico en la legislación de la firma electrónica, y que incluso cuenta con la Ley de Servicios de la Sociedad de la Información donde se tipifica la responsabilidad de los prestadores de servicios.

Comenzaré, por lo tanto con precisiones como "El consentimiento" y nos iremos adentrando en conceptos más profundos y concretos, a fin de conocer las redes de telecomunicaciones y hasta dónde nos puede llevar la tecnología. Por esto, el lector encontrará conceptos y términos en inglés, que no tienen una adecuada (y reconocida) traducción al español.

CAPÍTULO I
EL CONSENTIMIENTO

SUMARIO.- 1.1 Concepto de consentimiento 1.2 Formas en que se puede manifestar el consentimiento 1.3 La formación del consentimiento entre no presentes 1.4 Formación del consentimiento entre presentes 1.5 El consentimiento en los contratos por adhesión 1.6 Los contratos electrónicos y la legislación mexicana. 1.7 La fe pública del notario ante los medios electrónicos.

1.1.Concepto de consentimiento

La palabra consentimiento es utilizada jurídicamente como un elemento de existencia de los contratos, siendo así un requisito que el contrato debe de contener, para producir la eficacia del acto jurídico.

Para que se forme el consentimiento se necesitan dos emisiones de voluntad sucesivas, como la oferta y la aceptación que a su vez le dan la existencia a este elemento. Lo más importante del consentimiento es determinar el momento en que se otorgan estas dos declaraciones de voluntades, ya que a partir de que surja éste, nacerá el contrato y sucesivamente podrá producir sus efectos legales.

Carlos Enrigue Zuloaga[1] manifiesta que la voluntad en el campo de lo jurídico tiene que ir encaminada a producir frutos de justicia por medio de la realización de actos jurídicos, de tal modo que la voluntad determinará el actuar hacia la obtención de este bien. Así, el consentimiento se inicia con la exteriorización de la oferta que conocida por aquél o aquéllos a quienes se dirigió, es aceptada y con ello, se da el consentimiento, es decir que existe un acuerdo de voluntades de dos o más personas con el fin de lograr efectos de derecho.

[1] ENRIGUE, Carlos. *Pacto Contractual y Contratos Atípicos*, Porrúa, México 2000, p.8.

Sin llegar muy a fondo al concepto del consentimiento podemos deducir que el consentimiento se forma por la oferta y la aceptación; ahora, hay que tener muy en cuenta el momento en que se forma el consentimiento y si éste a su vez puede ser de una manera tácita o expresa:

a) La expresa consiste en una manifestación ya sea de palabra, escritura, por medios electrónicos, ópticos o cualquier otro tipo de tecnología o signos inequívocos y
b) La tácita, a diferencia de la expresa, se exterioriza por una conducta que autorice a inferir de ella la intención o la voluntad de contratar. [2]

A diferencia de las maneras tácita y expresa en las que puede el consentimiento concretarse, el silencio no es una manifestación de la voluntad, por lo tanto no puede deducirse del mismo una propuesta o aceptación de la oferta.

El doctrinista Manuel Bejarano[3] expresa que el silencio presenta un significado equívoco y por mucho que se deseche el formalismo, el consentimiento necesariamente ha de demostrarse. Cuando ante una propuesta sólo reaccionamos manteniendo silencio, no puede decirse que hemos aceptado y por tanto no hay contrato. No obstante, hay situaciones en que el acto parece integrarse por efectos del silencio, pero en ellas no es el silencio, sino los hechos que lo acompañan, lo que demuestran la voluntad de contratar.

De lo anteriormente expuesto puedo deducir que la formación del consentimiento generalmente se lleva a cabo mediante una oferta seguida de una aceptación lisa y llana, pero hay veces que esto no puede darse ya que existen negocios importantes en los cuales se abre un proceso de negociación entre una y otra, que frecuentemente hace que varíen los términos de la primera oferta, en este tipo de negociaciones podemos dar un ejemplo muy claro de lo que es el contrato de adhesión donde el oferente fija todos y cada uno de los elementos y el aceptante sin más, acepta la oferta naciendo entonces el contrato.

---

[2] *Código Civil Federal*, Ediciones Fiscales Isef, Edo. México, 2004. p. 188.
[3] BEJARANO SÁNCHEZ, Manuel, *Obligaciones Civiles*, Oxford University Press, México, 1998, p.55.

Para que se produzca un acto jurídico tienen que darse dos tipos de elementos: de existencia y de validez. Como lo vimos en el párrafo anterior, los elementos de existencia de un acto jurídico son el consentimiento y el objeto, en cambio los elementos de validez son: la capacidad de las partes, la ausencia de vicios de la voluntad, el cumplimiento de la forma legal y la licitud en el objeto motivo y fin, por lo que a continuación analizaré sólo algunos de los elementos de validez que considero más importantes para el tema que deseo tratar.

A) **Capacidad de los contratantes**: El Código Civil Federal en su artículo 1798 dice claramente: "son hábiles para contratar toda las personas no exceptuadas por la ley", lo que significa que cualquier persona podrá ser capaz mientras que no se encuentre en alguno de los casos previstos por la ley en los que aparecen como incapaces para contratar.

Este elemento de validez es de suma importancia para que el consentimiento se pueda dar ya que si no tenemos capacidad para contratar, nuestro acto jurídico tendrá una nulidad relativa.

El doctrinista José Luis de la Peza[4] explica que la capacidad es la regla y la incapacidad es la excepción, "Toda persona es capaz para contratar y obligarse, salvo que se encuentre en uno de los supuestos de incapacidad que expresamente establezca la ley".

La ley establece en el articulo 450 del Código Civil Federal la incapacidad de manera general y algunos ejemplos de ésta son: los menores de edad, los mayores de edad que presenten cierta disminución de inteligencia, o aquéllos que hayan sido atacados por alguna enfermedad que los haya dejado mal, tanto física, psicológica o sensorialmente.

[4] DE LA PEZA, José Luis, *De las Obligaciones*, Mc Graw Hill, México, 1999, p. 27.

También podemos encontrar incapacidades especiales, como aquellos actos jurídicos que no pueden realizar personas que estén en ciertos cargos de gobierno; un ejemplo de esto son los magistrados, jueces, peritos etcétera, que intervengan dentro de un juicio, no pueden comprar los bienes que son objeto del mismo.

En los artículos 22, 23, 486-489 del Código Civil Federal se puede interpretar que la falta de capacidad de ejercicio puede suplirse mediante la persona que está a cargo del cuidado de los intereses del incapaz, esta persona puede ser quien ejerce la patria potestad o tutela y en algunos casos la autoridad judicial será quien nombre al tutor, en tanto que la legitimación es la específica posición de un sujeto respecto de ciertos bienes o intereses, por lo que su declaración de voluntad puede ser operante respecto de estos. Es una particular relación del sujeto con el objeto del negocio o de otro acto jurídico[5]

B) **Ausencia de vicios**: las partes que celebran un acto deben otorgar su voluntad de una forma cierta y libre, consciente y en igualdad de circunstancias. Por vicios del consentimiento se pude entender que son las circunstancias que impiden que la voluntad de contratar sea libre y por lo tanto válida; estos vicios del consentimiento son:

1) *El Error*: este vicio se da cuando uno de los contratantes o ambos se han formado un concepto equivocado o juicio falso sobre la realidad. El error puede existir, sin ser determinante de la voluntad; esto significa que el acto conserve su validez cuando se da sobre cualidades accidentales, y éste es el caso en que se da derecho a indemnización o cuando el error es de cálculo sólo se da derecho a que se rectifique.

El error puede ser de hecho o de derecho; el error de derecho consiste en un concepto equivocado sobre la naturaleza o efectos jurídicos del contrato; en cambio el de hecho recae sobre las circunstancias fácticas, de hecho, del contrato que se va a celebrar. El error de derecho no debe afectar la validez del contrato, sin embargo el artículo 1813 del Código Civil Federal ataca la validez del contrato por error de derecho, el artículo se refiere al error de derecho o de hecho invalidando al contrato cuando este error recae sobre

[5] *Código Civil Federal, Op.cit.* p. 64

el motivo determinante de la voluntad de cualquiera de los que contratan y si en el acto de la celebración se declara ese motivo o se prueba, el juez juzgará sobre el alcance de dicho error.

El error de hecho sólo vicia la voluntad, en cambio el error obstáculo impide el consentimiento. Se puede encontrar otros tipos de error denominados error dirimente o error obstáculo:

a) Error *in corpore*, recae sobre el objeto.
b) Error *in negotio*, recae sobre la naturaleza del contrato a celebrar.
c) Error *in persona*, recae sobre la persona del contratante.
d) Error *in substancia*, recae sobre cualidades esenciales de la cosa, sobre el motivo determinante de la voluntad de cualquiera de las parte que contratan, este tipo de error es denominado como un error de nulidad. Este tipo de error no se impide el consentimiento, sin embargo está viciado y produce una nulidad relativa.

Estos errores sólo son dirimentes cuando se tratan de contratos *intuitu personae*[6]

Existen los errores que no impiden la formación del consentimiento ni tampoco dan lugar a la anulación del contrato, sino solamente a su rectificación:

a) Error *in quantitate*: es sobre la cantidad.
b) Error *in qualite*: sobre las cualidades de la cosa.
c) Error *in diferente*: este recae sobre motivos no determinantes de la voluntad o sobre cualidades secundarias del objeto.

2) El Dolo: este vicio tiene un elemento principal que es lo que distingue al dolo de los demás elementos. El artículo 1287 del Código Civil de Jalisco señala: "Hay dolo cuando

[6] Los contratos *intuitu personae* son aquéllos en los que el motivo determinante de la voluntad de las partes es la calidad de las personas con las que se contrata, por ejemplo, el mandato.

se emplea cualquier artificio para inducir al error"[7]; sin embargo el artículo 1815 del Código Civil Federal describe el dolo en los contratos como cualquier sugestión o artificio que se emplee para inducir al error o mantener en él a alguno de los contratantes. Podemos ver la similitud de ambas definiciones ya que las dos mencionan el hecho de inducir al error, aprovechándose de la ignorancia de la otra persona, sin embargo estas definiciones no están completas puesto que no se menciona detalladamente el concepto de dolo. Si nos remitimos a otro tipo de legislación podemos encontrar más a fondo dicho concepto. Aquí considero más acertada la definición del Código Civil español: "Hay dolo cuando, con palabras o maquinaciones insidiosas de parte de uno de los contratantes, es inducido el otro a celebrar un contrato que, sin ellas, no hubiera hecho".[8]

Los legisladores mexicanos hacen una pequeña diferencia entre lo que es la mala fe y el dolo, considerando a la mala fe como una disimulación del error de uno de los contratantes, de una forma más clara; para que el contratante dé su consentimiento para llevar a cabo el contrato, la contraparte a sabiendas de que existen deficiencias dentro del objeto del contrato hace caso omiso de ello, para pasarlo por inadvertido, y así la otra parte contratará sin saber del error que tiene el contrato. Otro de los elementos del dolo es el engaño; éste impulsa a celebrar un contrato para hacerle aceptar condiciones distintas de las que hubiere aceptado si no hubiera sido engañado. Por último hay que señalar que el dolo es causa de nulidad, así como el error cuando afecte a la causa determinante del consentimiento.

3) La violencia o intimidación; la violencia es un aspecto meramente físico que repercute, ya sea directa o indirectamente, en el consentimiento. La persona se puede ver atacada o amenazada ante determinado acto y actuar en consecuencia en contra de su voluntad, incluso sin tener deseo de llevar a cabo el acto en sí. Los doctrinistas y los legisladores deberían de aportar una definición más a fondo donde se hable de la violencia tanto física como violencia de la voluntad que repercutan en lo jurídico.

---

[7] *Código Civil para el Estado de Jalisco*, Porrúa, México, 1998.
[8] *Código Civil*, Editorial Aranzadi, Madrid, 1993.

La definición de violencia o intimidación dada por el Código Civil Federal[9] es: "Hay violencia cuando se emplea fuerza física o amenazas que importen peligro de perder la vida, la honra, la libertad, la salud o una parte considerable de los bienes del contratante, de su cónyuge, de sus descendientes, de sus ascendientes o de sus parientes colaterales dentro del segundo grado." Esta definición es criticable ya que de manera específica menciona los elementos que deben de darse para que exista la violencia pero si no se da ninguno de los elementos que se mencionan en el Código Civil Federal, entonces ¿estaríamos hablando de violencia o no?. Por esta razón considero que el punto, de si se incurrió o no en violencia debería dejarse al libre arbitrio del juez. Ahora si nos enfocamos a la definición que da el Código Civil para el Estado de Jalisco podríamos decir que es una definición más abierta: "...cuando se emplee fuerza física cualquiera o moral que causen en la víctima el temor de perder o sufrir menoscabo en algunos de sus bienes".[10] Está definición supera a la que nos da el Código Civil Federal, sin embargo todavía le hace falta en la redacción del artículo, en donde habla de ".....se empleé fuerza física.....", que también nos mencionara "la voluntad". ¿En que afectaría jurídicamente? El Código Civil español define: "Hay violencia cuando para arrancar el consentimiento se emplea una fuerza irresistible"[11]; esta definición utilizada por el legislador español la considero óptima, ya que cualquier elemento que se utilizara para arrancar o viciar el consentimiento se tomaría como violencia. En resumen lo que causa la violencia es el temor o el miedo y esto es lo que vicia al consentimiento, pero hay que estar de acuerdo en que este miedo o temor no deben de ser simples sino graves, que no sea un temor supersticioso, sino que sea real e inminente, que sea injusto y que no sea provocado por la víctima.

4) La lesión: es el perjuicio que una de las partes experimenta a consecuencia de un acto jurídico que se celebró con desproporción exagerada de las prestaciones de alguna de las partes. El legislador en el estado de Jalisco estableció la posibilidad de elegir por la parte

---

[9] *Código Civil Federal, Op. cit.* p.189
[10] *Código Civil para el Estado de Jalisco, Op. cit.* p. 12.
[11] *Código Civil, Op. cit.* p. 13.

ofendida, la nulidad del contrato o la reducción equitativa de su obligación, en ambas se establece la posibilidad de cobrar daños y perjuicios.

1.2. Formas en que se puede manifestar el consentimiento

Nuestro Código Civil Federal, adopta como una forma de manifestar el consentimiento la consensualidad y la formalidad como una excepción: "Los contratos se perfeccionan por el mero consentimiento". La ley no obliga a los contratos civiles a revestir cierta forma, sino que cada contrayente se obliga de la manera y términos que le parezca, sin que para la validez del contrato, se requiera de una forma determinada, fuera de los casos en que la ley así lo exija.

La ley exige una forma determinada para los documentos escritos, entre los que se encuentran:

a) El escrito privado que consiste únicamente en un documento firmado por las partes.
b) El escrito privado firmado ante dos testigos.
c) El escrito privado y ratificado ante fedatario público; en este caso la ratificación, no lo quita el que sea un documento privado, ya lo único que hace el fedatario es verificar la autenticidad de las firmas.
d) La escritura pública, este documento se asienta en el protocolo de un notario público con la participación y la asistencia de éste.

Cuando la ley nos exija la forma escrita en cualquier acto jurídico también podrá ser aplicable la utilización de medios electrónicos, ópticos o cualquier otra tecnología siempre y cuando se pueda atribuir a la persona y consultar el artículo 1834 Bis del Código Civil Federal.

En la vida cotidiana aunque muchas veces la ley no especifique la forma de un contrato, los contratantes siempre buscan la tranquilidad por lo tanto hacen constar el contrato por escrito, ya sea para sentir cierta seguridad, o para tener en que apoyarse en caso de incumplimiento o para hacerlo valer como prueba; sin embargo con las reformas que se hicieron al Código Civil Federal y al Código de Comercio, los contratantes pueden valerse de medios electrónicos, ópticos o de cualquier otra tecnología para realizar un acto jurídico y siendo este perfectamente válido, nos encontramos ante ciertas cuestionantes: ¿Es seguro el acto? ¿Es eficaz? ¿Realmente produce los efectos como cualquier otro contrato? Este tipo de cuestiones las explicaré en el transcurso del presente trabajo.

De entrada hay que aclarar la diferencia que existe entre un documento constitutivo y un documento probatorio. Un documento constitutivo es aquel documento que es necesario para la validez de un contrato. Los documentos meramente probatorios son aquéllos que no son necesarios para la validez ni para la eficacia del contrato.

En aquellos casos en que la ley exige determinada forma para los contratos a fin de que sean válidos y las partes deciden llevarlo a cabo sin esa forma, el artículo 1833 del Código Civil Federal le da la facultad a las partes de llevarlo a cabo, aun sin que revista la formalidad, dado que la ley dice ".....Pero si la voluntad de las partes para celebrarlo consta de manera fehaciente, cualquiera de ellas puede exigir que se dé al contrato la forma legal."[12] Si nos damos cuenta del error tan grave que tiene este artículo, ya que se contradice, nos podemos encontrar con el problema de que alguna de las partes quiera demandar la nulidad del contrato, por falta de forma, y en este caso el juez tendría que resolver a favor de quién demanda el otorgamiento de la forma, ya que el artículo 2229 del Código Civil Federal[13] expresamente dice que "la acción y la excepción de nulidad por falta de forma compete a todos los interesados."

---

[12] *Código Civil Federal, Op. cit.* p. 14.
[13] *Idem.*

1.3. La formación del consentimiento entre no presentes

Existen varias teorías acerca de cuándo se debe de considerar integrado el acuerdo de voluntades cuando se trata de algún tipo de comunicación mediato (carta, telegrama, y teléfono son la excepción ya que son medios inmediatos).

1) *Teoría de la declaración.* En ésta el consentimiento se manifiesta en el momento que el destinatario recibe la oferta y está conforme con ella y declara en cualquier forma aceptarla.
2) *Teoría de la expedición.* Aquí no basta con la simple aceptación, hay que hacer una manifestación de la voluntad de forma clara. Es el caso de la carta donde se expresa la aceptación y es depositada en el correo.
3) *Teoría de la recepción.* Ésta consiste en que el pacto se perfecciona cuando el oferente recibe la aceptación.
4) *Teoría de la información.* El consentimiento se otorga cuando la oferente conoce de la aceptación, es decir se informa de ella.

1.4. Formación del consentimiento entre presentes

Una vez que tenemos la oferta y la aceptación para que se forme el consentimiento entre presentes se pueden dar las siguientes hipótesis:

b) *Oferta sin fijación de plazo.* Esta hipótesis es el caso de una aceptación inmediata, cuando el oferente ofrece la oferta e inmediatamente queda aceptada el oferente se encuentra obligado. Por otro lado, si el oferente ofrece la oferta y la aceptación no se hace inmediatamente, aquél no queda obligado. El artículo 1805 del Código Civil Federal[14] establece:

[14] *Idem.*

"Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla el autor de la oferta quedará desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono".

c) *Oferta con plazo*. En esta hipótesis el oferente queda ligado de su oferta hasta que expire el plazo que haya dado para la aceptación de la misma.

d) *Oferta por teléfono*. Éste es un medio simultáneo, por lo tanto se refiere a que esté presente una persona en el momento que se hace la oferta. El código de Jalisco lo regula como una oferta entre presentes, si no hay una aceptación simultánea al momento de la oferta el oferente no se encontrará obligado, así mismo conforme al Código Civil Federal en el artículo 1805[15], cuando se trate de una oferta a través de un medio electrónico, óptico o de cualquier otra tecnología se entiende que es una oferta de aceptación inmediata y que al igual que la oferta hecha por teléfono se entiende desligado el oferente si la aceptación no fue hecha inmediatamente.

e) *Casos en que el oferente queda libre de su oferta*. El artículo 1278 del Código de Jalisco[16] dice que la aceptación deberá ser lisa y llana para que el oferente quede obligado, por esto se entiende que no implique ninguna modificación a la oferta, este es el caso de cuando el oferente deja de serlo para convertirse en aceptante y el aceptante en oferente, es decir cuando se cambian los papeles a la hora de llevar a cabo una oferta. El artículo 1810 del Código Civil Federal[17] refiere: "El proponente quedará libre de su oferta cuando la respuesta que reciba no sea una aceptación lisa y llana, sino que importe modificación de la primera."

---

[15] *Ibid.* p. 9.
[16] *Código Civil para el Estado de Jalisco Op. cit.* p. 12.
[17] *Código Civil Federal Op. cit* p. 14.

1.5. El consentimiento en los contratos por adhesión

Algunos autores hacen la distinción entre contratos por adhesión y contratos de adhesión, al respecto De Buen Lozano[18] nos dice: "El contrato por adhesión, trata de implicar un modo de contratar, y la segunda una clase especial de contrato".

El doctrinista Ricardo Uribe-Holguín[19] define al contrato de adhesión como aquél que "se celebra mediante la libre discusión, en que una de las partes tiene preparada una oferta inmodificable que la otra ha de aceptar o rechazar sin posibilidad de contra-proposición, mientras que en la oferta inmodificable, el acuerdo de voluntades se forma previa discusión de todas las estipulaciones o de las más importantes."

La pregunta que debemos hacernos en estos contratos es ¿dónde se encuentra el consentimiento? o ¿en qué momento debe de otorgarse?

Borja Soriano[20] nos dice al respecto: "La oferta se hace a una colectividad; el convenio es obra exclusiva de una de las partes; la reglamentación del contrato es compleja; la situación del que ofrece es preponderante; la oferta no puede ser discutida; el contrato oculta un servicio privado de utilidad pública". Podemos agregar que un contrato por adhesión usualmente debe ser aprobado por el estado ya que hay una utilidad pública de por medio y que encima de esto se deben de determinar las tarifas del servicio que sea objeto del contrato. Por citar algunos ejemplos de contratos de adhesión, podríamos decir que se encuentran los de energía eléctrica, el servicio telefónico, telégrafos, el transporte terrestre, el contrato de seguro, algunos contratos bancarios (no todos), depósitos de dinero, etcétera.

---

[18] DE BUEN LOZANO, Néstor. *La decadencia del contrato*, Textos Universitarios, S.A., México, DF., 1965, p. 294.
[19] URIBE-HOLGUÍN Ricardo, *Cincuenta breves ensayos sobre Obligaciones y Contratos*, Editorial Temis, Bogotá, Colombia, 1970, p. 171.
[20] BORJA SORIANO, Manuel, *La évolution technique du contra*, número 15, pp. 48-49.

La justificación que le encuentran algunos autores a este tipo de contratos de adhesión es la cantidad de transacciones que se hacen diariamente en la vida cotidiana de las personas, ya que no habría tiempo suficiente para pararnos a discutir para llegar a un acuerdo de una mejor oferta. El ejemplo más simple que puede haber es el de un estacionamiento: la mayoría de la gente que tiene carro, al menos una vez a la semana utiliza un estacionamiento y lo quiera o no, se tiene que obligar a las condiciones que el estacionamiento le impone a la hora de entrar y en este caso no hay manera de dar marcha atrás (a menos de que no lo utilizáramos).

En el caso del contrato de adhesión, el consentimiento lo podemos ver claramente cuando se nos hace una oferta que está latente para todo el público; nosotros podemos elegir entre aceptarla o no. Volviendo al ejemplo del estacionamiento ¿queremos estacionarnos? ¿ese es el objeto del contrato? que nos presten un servicio que necesitamos en ese momento, el oferente hace su oferta y nosotros podemos o no aceptarla es así de sencillo optamos por entrar al estacionamiento o no, ahí podemos ver claramente el consentimiento, por lo tanto el contrato de adhesión es un contrato, y lo es por que hay consentimiento, y el consentimiento no supone necesariamente el derecho a discutir, mientras la oferta pueda aceptarse o rechazarse, la voluntad actúa regularmente lo que no obsta para que obre mejor cuando haya habido discusión.

Nuestra legislación denomina a estos contratos de adhesión. El artículo 1858 del Código Civil Federal [21] y el artículo 1328 del Código Civil para el Estado de Jalisco[22] mencionan que: "Los contratos que no estén especialmente reglamentados en este código, se regirán por las reglas generales de los contratos, por las estipulaciones de las partes y, en lo que fueren omisas, por las disposiciones del contrato con el que tengan más analogía, de los reglamentados en este ordenamiento."

Un contrato de adhesión es un contrato *standard* pero no todo contrato *standard* es un contrato de adhesión, condiciones idénticas para todos los que contratan bajo estas

[21] *Código Civil Federal Op. cit.* p. 9.
[22] Código Civil para el Estado de Jalisco. *Op. cit.* p. 12.

cláusulas y la mayoría de las cláusulas no están sujetas a negociación.[23] Aunque de cierta forma este párrafo nos puede dar a entender que se trata de un contrato de papelería o un formulario ya previsto y usado por la mayoría de la gente, tal como los contratos de arrendamiento, no es así ya que se encuentran sustentados para cada negocio en el que se puedan aplicar y no son generales, simplemente son especiales para los distintos fines que se le de al contrato de adhesión.

Al respecto, el autor González Palomino nos dice[24]: "No se trata de una cláusula formularia, ni sobreentendida, ni optativa, sino todo lo contrario, una cláusula estudiada, analizada previamente, de verdadero calor intelectual y de serio empleo instrumental."

Las razones más acertadas de por qué existe el contrato de adhesión es el ahorro económico ya que se aduce que si se logra la predisposición de cláusulas se producirá tal ahorro en éstos que beneficia, obviamente, al empresario y de manera evidente al consumidor, pues los precios de las mercancías bajarán al ser reducidos los costos. Podría establecerse también que el consumidor actual no tiene ni el tiempo ni los conocimientos para discutir al detalle los contratos y generalmente podría ser muy costoso asesorarse para celebrarlos. Sin embargo, tampoco es justificable que a cambio de otros beneficios puedan autorizarse precios abusivos, éste podría ser el caso de muchas empresas ya sea de energía eléctrica o teléfonos.

1.6. La legislación mexicana y los contratos electrónicos

La legislación mexicana en el Código Civil Federal en su artículo 1792[25]define al convenio como: "el Acuerdo de dos o más personas para crear, transferir, modificar o extinguir obligaciones." Y el artículo 1793 del mismo dice: "Los convenios que producen o transfieren las obligaciones y derechos toman el nombre de contratos". Entonces cuando llevamos a la práctica una operación dentro de la Web que transfiera obligaciones y

[23] Deutch, Sinai, según cita de Carlos Enrigue Zuloaga , *Unfair contracts*, Lexington Mass. 1977.
[24] GONZÁLEZ PALOMINO, José, *Instituciones de derecho notarial*, t. L., Madrid 1958.
[25] *Código Civil Federal. Op. cit.* p. 2.

derechos ¿estamos hablando de realizar un contrato a través de internet? Podría sonar muy lógico, que sin darnos cuenta del acto jurídico que estamos realizando en internet, hayamos llegado a la existencia de un contrato. Claro que hay que revisar que en este acto se den los elementos de existencia del contrato: el consentimiento y el objeto. El consentimiento, como ya lo vimos, a través de medios electrónicos se da inmediatamente ya sea de manera expresa vía mail, o tácita; el ejemplo de ésta puede ser a través de una compraventa en una página de internet, que con tan solo un clic aceptemos comprar el producto.

El objeto, que se regula en la legislación mexicana al igual que en internet, debe existir en la naturaleza, tiene que ser determinable en cuanto a su especie y estar dentro del comercio; si no se cumplen estos requisitos se da la nulidad absoluta del contrato.

Cuando hago referencia a un contrato que se lleva a cabo de forma electrónica, me estoy refiriendo a un contrato electrónico, que podría definirse como: "aquél que se realice mediante la utilización de algún medio electrónico que conlleva a exteriorizar el consentimiento para transmitir derechos y obligaciones".

En cambio los contratos informáticos son instrumentos jurídicos que han ido evolucionando con la tecnología. Julio Téllez Valdés[26] define los contratos informáticos como "transacciones de bienes y servicios que se hacen a través de la tecnología informática." La definición más explícita la da Willheim David Angermüller[27]: "Es el acuerdo de voluntades de dos o más partes con el objeto de crear vínculos de obligaciones y que busca crear, regular, modificar o extinguir una relación jurídico patrimonial." Algunos ejemplos de estos contratos son los de compraventa de hardware y de software, leasing y renting, licencias de uso y acuerdos de desarrollo de programas y los contratos de servicios que son aquéllos que se dan para la prestación de servicios informáticos, telemáticos y de información, etcétera.

[26] TÉLLEZ VALDÉZ, Julio. *Derecho Informático*. Editorial Mc Graw Hill, México 2004, p. 115.
[27] *Idem.*

El contrato informático va encaminado a la prestación de servicios que tenga que ver con equipos de cómputo, así como los elementos que conforman las computadoras, como los bienes informáticos. En cambio el contrato electrónico puede ser cualquier tipo de contrato regulado por nuestra legislación, sólo que se lleve a cabo de manera electrónica y que tenga relación directa con el consentimiento a través de la vía electrónica o el objeto del contrato se dé electrónicamente.

Hago la distinción de los conceptos electrónica, informática y telemático, a manera de que quede mejor expresada la diferencia entre los contratos electrónicos y los contratos informáticos.

1) *Electrónica:* es todo lo relativo al electrón, es el estudio del comportamiento de los electrones en diversos medios, como el vacío, los gases, y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos.[28] Refiriéndonos específicamente a los contratos electrónicos Davara Rodríguez explica que la contratación electrónica es aquélla que se realiza mediante la utilización de algún elemento electrónico cuando éste tiene o puede tener una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo.[29]

2) *Informática:* según Davara Rodríguez[30] "es la Ciencia del Tratamiento automático de información con las posibilidades que ofrece de almacenamiento y tratamiento de la documentación y la recuperación de la información registrada en soportes magnéticos, ópticos, u otros, permite controlar la información y puede llegar a convertirse en un instrumento de presión y control social."

La Real Academia de la Lengua Española define a la informática como el "conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automático de la información por medio de ordenadores".[31]

---

[28] *Idem.*
[29] DAVARA RODRÍGUEZ, Miguel Ángel. *Manual de Derecho Informático*, 5ª ed, Editorial Aranzadi, Madrid 2003, p.194
[30] *Ibid.* p.46.
[31] *Diccionario de la Lengua Española*, Real Academia Española, Espasa Calpe, España, 2002.

Julio Téllez Valdés[32] lo define como el "conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información." Por lo anterior puedo deducir que la informática no es más que el cúmulo de información que se reproduce a través de ordenadores.

La informática debe de estar regulada por el derecho, por lo que se toma el nombre de derecho informático, pero según opinión de Davara Rodríguez este término se ha quedado obsoleto ya que no se trata solamente de regular la informática sino a lo más actualizado hoy en día que es el derecho de las tecnologías de la información y las comunicaciones.

3) *Telemática:* es la conjunción informática y la aplicación de las técnicas de la telecomunicación y de la informática a la transmisión a larga distancia de información computarizada.[33] Davara Rodríguez[34] lo define como "Término fruto de telecomunicaciones e Informática que hace referencia al diálogo a distancia entre equipos informáticos."

De estas definiciones puedo deducir que son los medios por los cuales tenemos acceso a llevar a cabo cualquier acto ya sea jurídico, económico o comercial, a través de medios electrónicos.

En cuanto a la forma de estos contratos, tanto informáticos como electrónicos, el Código Civil Federal[35] en el artículo 1834 Bis, señala que cuando se exija la forma escrita para el contrato, se tendrá por cumplido en cuanto a forma, "...mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología y siempre y cuando se le pueda atribuir a las partes..."; en este artículo por primera vez se hace mención al fedatario público. Cuando la ley establezca que un acto jurídico debe de otorgarse en instrumento

---

[32] *Idem.*
[33] *Idem.*
[34] DAVARA RODRÍGUEZ, Miguel Ángel, *Op. cit. p.* 23.
[35] *Código Civil Federal. Op. cit.* p. 2.

ante fedatario podrá hacerse a través de medios electrónicos, ópticos o cualquier otra tecnología pero el fedatario público tendrá que verificar si es atribuible esa información a las partes y conservar bajo su resguardo una versión íntegra sobre la misma para su ulterior consulta.

Los notarios tendrán que tener mucho cuidado con el artículo 184 bis ya que les cambia por completo el contexto de su trabajo; una de las principales funciones de un notario es la capacidad de dar fe para hacer constar actos, negocios y hechos jurídicos a los cuales se les tiene que dar autenticidad y seguridad jurídica conforme a las leyes.[36]

Cuando hago referencia a contratos electrónicos surgen planteamientos como:

a) ¿Quién es responsable del mal funcionamiento de los sistemas electrónicos o de la transmisión de la información?

En este tipo de planteamiento hago referencia a las empresas que se encargan de proveer servicios vía electrónica, y en este supuesto hay que verificar si las empresas que llevan a cabo estos servicios son responsables del mal funcionamiento de los sistemas electrónicos; el tipo de responsabilidad imputable sería la responsabilidad civil y en este caso se podría demandar por daños y perjuicios.

b) ¿En qué momento y en qué lugar se perfecciona el contrato?

Lo primero que hay que verificar es la naturaleza del contrato, qué tipo de contrato se está llevando a cabo, si es de materia civil o mercantil. Segundo, ver si es un contrato sometido a un régimen internacional, ya que si es así, influye mucho el régimen que es aplicable; si es un régimen local el contrato se perfecciona por el mero consentimiento. El Código Civil Federal[37] en su artículo 1796 y 1811, segundo párrafo, dice: "Tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier

[36] *Ley del Notariado para el Estado de Jalisco*, Editorial Paco, Guadalajara, Jal., 2004.
[37] Código Civil Federal, *Op. cit.* p.9.

otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos". Por lo que se deduce que la oferta y la aceptación a través de estos medios, se entenderá inmediata y se perfeccionará el contrato al momento de su aceptación.

c) ¿En caso de que se suscitara un problema cómo podríamos probar las declaraciones que se emitieron por vía electrónica?

Esta pregunta va encaminada a probar la autenticidad, integridad, confidencialidad y no repudiación de los mensajes; todo esto nos puede servir como prueba, siempre y cuando utilicemos el sistema de la clave pública, el cual explicaré detenidamente más adelante. Por lo pronto lo que nos interesa para demostrar en juicio este sistema electrónico es primero el reconocimiento jurídico de los medios electrónicos, la manifestación de la voluntad a través de medios electrónicos que ya está vigente tanto en el Código Civil Federal como en el Código de Comercio, el reconocimiento como valor probatorio de los mensajes de datos, que se registre el acto de comercio que se llevó a cabo y que se proteja al consumidor. Todo esto nos sirve para probar en juicio que se llevó a cabo un acto jurídico a través de medios electrónicos.

1.7. La fe pública del notario ante los medios electrónicos

Jorge Ríos Helling[38] dice: "El notario como parte del notariado de corte latino se encarga de interpretar la voluntad de las partes y plasmar ésta en un documento público y auténtico que puede ser una escritura pública, si se trata de dar fe de un acto jurídico o bien un acta notarial si se certifica un hecho jurídico material." El notario es uno de los fedatarios que más amplias facultades tiene, por esta razón lo menciono, ya que en el proceso de firma electrónica el notario toma mucha importancia porque tiene fe pública y como lo vimos en el párrafo anterior, es el notario el encargado de dar fe al acto jurídico que se lleva a cabo por medios electrónicos.

[38] RÍOS HELLING, Jorge, *La Práctica del Derecho Notarial*, Mc. Graw Hill, México, 2002. p. 50

El artículo 45 de la Ley del Notariado para el Distrito Federal,[39] señala la única prohibición que tiene el notario, respecto de sus funciones, "...dar fe de actos que dentro de los procedimientos legales respectivos corresponda en exclusiva hacerlo a algún servidor público, sin embargo sin tener en principio, ese valor procedimental exclusivo, sí podrán cotejar cualquier tipo de documentos, registros y archivos públicos y privados respecto a ellos u otros acontecimientos certificar hechos, situaciones o abstenciones que guarden personas o cosas relacionadas o concomitantes con averiguaciones, procesos o trámites, lo cual tendrá valor como indicio calificado respecto de los mismos, sujeto a juicio de certeza judicial y sólo será prueba plena con relación a aspectos que no sean parte esencial de dichas facultades públicas, aspectos que deberá precisar en el instrumento indicado." Menciono la Ley del Notariado para el Distrito Federal, ya que la Ley del Notariado para el Estado de Jalisco no menciona las prohibiciones a los notarios, las cuales considero de gran importancia conforme a lo que marca la ley.

El fundamento constitucional para que exista la figura del notario está en los artículos 121 y 124 de la Constitución Política de los Estados Unidos Mexicanos;[40] el artículo 122 de la misma es el fundamento para la Ley del Notariado para el Distrito Federal.

El artículo 26 de La Ley del Notariado para el Distrito Federal explica la naturaleza del notario, la cual es autónoma, pública y libre, porque se ejerce actuando con fe pública y ésta es otorgada a través de los poderes del estado, mientras que el artículo 13 menciona la fe pública mas no la define, sin embargo nos dice que se aplicará para cada caso en concreto.

Jorge Ríos Helling[41] dice que la fe pública está dirigida a una colectividad y es obligatoria, debe constar siempre en forma documental y el estado la tiene y crea con el fin de brindar seguridad jurídica; es por esta razón que se debe tener por cierto y verdadero lo

---

[39] *Ley del Notariado para el Distrito Federal*, publicada en la Gaceta oficial del Distrito Federal el 29 de enero del 2004.
[40] Constitución Política de los Estados Unidos Mexicanos, Ediciones Delma, México, 2004.
[41] RÍOS HELLING, Jorge, *Op. cit.* p. 26.

que emana de ella, y la define como "seguridad otorgada por el Estado para afirmar que un acto o hecho es verdadero".

Ahora hay que afirmar que esta fe pública de la que hago mención no es todavía la que el estado le otorga al notario, sino de la que el estado en un determinado momento le otorgará al notario, por lo que me pregunto: ¿La fe pública, no necesariamente tiene que estar asentada por escrito en un papel? ¿Existe opción de que esté por escrito o no? La ley no especifica muy claramente esto. De hecho hasta pueden surgir confusiones respecto al punto, por lo que mi siguiente pregunta sería: ¿El notario podrá dar fe pública sobre un documento electrónico, sin que éste medie en un papel por escrito?

Surge una disyuntiva ya que en el párrafo anterior hice mención a la fe pública pero cuando se habla de la forma de dación de fe del notario significa que es una fe delegada por el estado que es por escrito porque se tiene que materializar y por lo tanto es un elemento de validez de los actos jurídicos que si faltara produce nulidad relativa del acto; su fundamento legal lo encontramos en el artículo 1795 FCC. IV del Código Civil Federal[42] "...porque el Consentimiento no se haya manifestado en la forma que la ley establece." El artículo 1834 Bis del mismo Código, dice:

> 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 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 de cualquier otra tecnología en el propio instrumento los elementos a través de los cuales se guardó una versión íntegra de la misma para su ulterior consulta otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

[42] *Código Civil Federal, Op. Cit.* p. 9.

Esto significa entonces, que si llevamos a cabo un acto jurídico a través de un medio electrónico, en el cual el notario dará fe pública notarial, el mismo acto jurídico que se realizó de manera electrónica se asentará por escrito, si no es así entonces no se estaría materializando esta fe y en consecuencia se aplicaría el artículo 2232 del Código Civil Federal, donde se indica que por falta de forma el acto produce la nulidad, de tal manera que cualquiera de las partes podrá pedir que se le otorgue la forma que dicta la ley. Volviendo a las preguntas de los párrafos anteriores, si nos apegamos estrictamente a lo que dicta la ley, se deduce que no puede haber entonces una fe pública asentada a través de medios electrónicos porque causaría nulidad relativa del acto por falta de forma, la pregunta ahora sería: ¿Se materializa la fe pública notarial en medios electrónicos? Yo considero que sí y por lo tanto es perfectamente válida esa fe, sólo que a mi parecer ni en el Código Civil Federal[43] ni en el de Jalisco[44] ni en la Ley del Notariado[45] se encuentra bien redactada la forma en que se materializará la fe pública notarial, por lo cual preveo que surgirán problemas respecto a este tipo de regulaciones en materia civil.

Es el Código de Comercio[46] en el artículo 93 el que hace mención a la forma de los contratos y dice así: "Cuando la ley exige la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensajes de Datos, siempre que la información en el contenido se mantenga íntegra y sea accesible para su ulterior consulta...". Esto respecto a actos, convenios o contratos, ¿pero si estamos hablando de fe pública notarial también se equipara a este supuesto?

El tercer párrafo del mismo artículo dice:

> En los casos en que la Ley establezca como requisito que un acto jurídico debe 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

[43] *Idem.*
[44] Código Civil para el Estado de Jalisco, *Op. cit.* p.12
[45] *Ley del Notariado, Op. cit.*
[46] *Código de Comercio*, Ediciones Fiscales Isef, Estado de México, 2004.

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.

Este artículo del Código de Comercio es más claro que los artículos del Código Civil Federal, y en las primeras líneas del último párrafo da a entender que la fe notarial también se puede hacer a través de medios electrónicos, sin embargo si leemos el último renglón de este artículo nos daremos cuenta que dice: "...se otorgará dicho instrumento con la legislación aplicable que lo rige," y la legislación que lo rige es el Código Civil Federal. Aquí volvemos a la misma disyuntiva, será el juez, quien a su arbitrio se incline por aceptar la fe notarial a través de medios electrónicos, o quizá más adelante existan reformas a la ley que aclaren este punto en la legislación mexicana.

CAPÍTULO II
LOS CONTRATOS EN INTERNET

SUMARIO.- 2.1 Los Contratos informáticos 2.2 Antecedentes evolutivos de los contratos informáticos. 2.3 Los contratos relativos a internet 2.4 Formación de un contrato electrónico.

2.1 Los Contratos informáticos

El autor Pedro Alberto de Miguel Asensio[47] habla de los contratos electrónicos refiriéndose a internet como un medio para llegar al fin que se está persiguiendo a través del contrato realizado por medio de la Web; así mismo dice que los contratos electrónicos se perfeccionan mediante el intercambio electrónico de datos del ordenador, ya que sólo es uno de los medios de comunicación empleados para la formación de contratos de tal categoría. Un ejemplo muy claramente expresado es el del mercado de valores, ya que gracias a la difusión de internet se pueden dar esos contratos en ese mercado.

Miguel Asensio[48] también dice que la contratación electrónica trata de la transmisión inmaterial a través de redes informáticas de declaraciones negociables y la marginación de documentos en papel, el objeto de estos contratos puede recaer sobre un bien material cuya entrega física es necesaria para el cumplimiento, pues sólo en ocasiones se trata de prestaciones susceptibles de ser ejecutadas por medio de la transmisión a través de la propia red de información digitalizada.

En la legislación mexicana, en materia mercantil, todavía no se encuentran regulados los contratos informáticos, se hace mención a mensajes de datos en el Código de Comercio, o actos y convenios que se lleven a cabo a través de medios electrónicos, en el artículo 89, pero no regula de manera específica estos contratos.

---

[47] DE MIGUEL ASENSIO, Pedro Alberto, *Derecho Privado de Internet*, Civitas, España, 2001.
[48] *Idem.*

La manera en como se ha ido desarrollando internet ha llegado a crear grandes conflictos en cuanto a la manera de la contratación electrónica, cada vez son más los proveedores de servicios así como la gente que necesita de los mismos que la red puede proveer, por esta razón la contratación electrónica a través de internet demanda la adaptación del ordenamiento jurídico, que se trate precisamente de una red abierta y descentralizada. Puesto que en la transmisión a través de redes abiertas se multiplica el riesgo de que los datos sean manipulados por terceros, se exige que exista un normatividad para contratar a través de internet.

La aplicabilidad de las reglas generales a la contratación electrónica no resulta suficiente para garantizar la seguridad jurídica, ya que es difícil encontrar el momento de la perfección del contrato electrónico al momento de realizarlo a través de la red, tal y como lo había mencionado en el capítulo anterior, en supuestos en los que el ordenamiento exige requisitos de forma específicos, por ejemplo la forma escrita, esto puede conllevar la falta de confianza de los contratantes, debido a la falta de garantías sobre ciertos elementos, el caso de la identidad del contratante, prueba de la fiabilidad del contenido del contrato, etcétera. Por lo tanto para el desarrollo de la contratación por internet resulta necesaria la intervención legislativa que otorgue un marco jurídico fiable, con alternativas de que en caso de que no se produzca el cumplimiento pueda reclamarse ante tribunales el incumplimiento del contrato con las pruebas suficientes, y no que sólo quede flotando sobre la red, como si nunca se hubiera llevado a cabo un contrato de ese alcance, de aquí la importancia del notario para materializar la fe pública y poder probar que el acto jurídico se realizó.

En el plano internacional, numerosas organizaciones intergubernamentales como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI/ UNCITRAL)[49], la Organización para la Cooperación y el Desarrollo Económico (OCDE), y la Organización Mundial del Comercio (OMC), se han venido ocupando de la ordenación

[49] La Ley Modelo sobre Comercio Electrónico fue aprobada en 1996 y se modificó en 1998 por la Comisión de las Naciones Unidas para el derecho Mercantil Internacional (CNUDMI más conocida por UNCITRAL) por esta razón en este trabajo encontraremos las dos abreviaturas.

de los contratos electrónicos[50] El instrumento normativo tradicional para la elaboración de normas uniformes es el convenio internacional, su rigidez no se corresponde con las necesidades del tráfico, la rápida transformación tecnológica y el carácter descentralizado de internet, otras fuentes que también le pueden servir al legislador para el desarrollo del nuevo régimen legislativo, aunque carecen de eficacia, son la ley modelo, los códigos de conducta o las recomendaciones elaboradas por organizaciones internacionales.

A nivel internacional podemos encontrar mecanismos alternativos de unificación jurídica, caracterizados porque su eficacia no se subordina a la participación del legislador del país donde se lleva a cabo la contratación electrónica. La repercusión sobre el régimen jurídico del contrato de estas normas de origen extraterritorial, es mejor conocido como derecho internacional. Entre estas normas, ocupan un lugar destacado los usos comerciales, en tanto que prácticas generalizadas en cada sector del tráfico, así como cláusulas contractuales de utilización generalizada son objeto de recopilación por organismos como la Cámara de Comercio Internacional. El desarrollo de contratos modelo es similar al proceso de estandarización experimentado en materia contractual. UNIDROIT presenta una particular importancia respecto de los contratos comerciales internacionales, ya que incorpora un elaborado compendio de reglas propias de la parte general del régimen de las obligaciones contractuales y presenta carácter no vinculante. Conforme a su preámbulo las situaciones más importantes en las que se prevé que operen los principios son: cuando así se acuerde entre las partes en el contrato, cuando se prevea que el contrato quede regido por la *lex mercatoria*, si no es posible determinar la regla aplicable al contrato, para interpretar o suplementar textos de derecho uniforme y por último, como modelo para la legislación a nivel nacional o internacional. También debemos tomar en cuenta el arbitraje como un importante papel en la consolidación y desarrollo de las reglas que integran ese conglomerado llamado *lex mercatoria*, unido a la creciente difusión del contenido de los laudos.

[50] SOERIEULF, R., *Brief Overview of International Initiatives for an Electronic Comerse Uniform Legal Framework*, URL, 1999.

2.2. Antecedentes evolutivos de los contratos informáticos

2.2.1 El surgimiento de internet

La internet es una red abierta donde cualquier persona puede participar, teniendo acceso a una línea telefónica y a un ordenador, se le considera a internet un elemento de la sociedad de la información[51], facilita los servicios electrónicos interactivos y la comunicación de todo tipo de información ya sean textos, sonidos, imágenes, videos, etcétera.

Técnicamente internet está constituida de una multiplicidad de redes a nivel mundial conectadas entre sí de un modo que hace posible la comunicación casi instantánea desde cualquier ordenador de una de esas redes a otros, situados en otras redes del conjunto, por lo que se trata de un medio de comunicación global. La conexión puede llevarse a cabo de diferentes maneras ya sea por cable coaxial, fibra óptica, líneas telefónicas, microondas y satélites.

Como dato cultural una red telemática es un conjunto de ordenadores conectados entre sí de manera que puedan comunicarse y compartir datos y recursos[52].

Los orígenes de internet se encuentran en la creación del ARPANET en 1969, una red de ordenadores que se creó para experimentar por la Agencia de Proyectos de Investigación Avanzada (Advanced Research Proyects Agency o ARPA)[53] del Departamento de Defensa de Estados Unidos, con el objetivo de establecer una red informática de comunicación que tuviera la capacidad de redirigir automáticamente la información, y a su vez esta información dividirla en paquetes, a fin de asegurarla para que pudiera llegar a su destino, evitando las partes de la red colapsadas. Al tiempo que sale esta red, comienzan a aparecer otras redes semejantes que facilitaron la conexión entre

---

[51] Comprende el uso masivo de las tecnologías de la información y comunicación, para difundir el conocimiento y los intercambios en una sociedad., Ríos Helling, Jorge, *Op. cit.* p. 26.
[52] *Ibid.* p. 30.
[53] CASTELLS, M. *La Galaxia Internet*, Traducción de R. Quintana, revisada por el autor, Madrid, 2001. p. 32.

universidades, centros de investigación, empresas y particulares a nivel mundial y fueron conectándose entre sí. Internet es la interred que conecta la mayor parte de las redes que existen en el mundo.

La internet funciona gracias al uso masivo de todas las personas que acceden a este servicio, así como a los operadores de sistemas informáticos, de redes y de protocolos comunes que operan en aquél. Es por estos medios que se permite el intercambio de datos y operaciones a ordenadores con total exactitud de información digital.

La forma de comunicación de internet es a través de la utilización del protocolo TCP/IP. El protocolo Transmisión Control y Protocolo (TCP) hace posible la división de la información en paquetes y la numeración de éstos para que puedan ser unidos en el orden correcto, en el ordenador de destino, al tiempo que incorpora los datos necesarios para la transmisión y la descodificación de los paquetes. Por otra parte el protocolo IP (Internet Protocol) se ocupa de que cada paquete sea etiquetado con las direcciones o números adecuados.

Los paquetes en que los protocolos dividen toda la información circularán para llegar a su destino por una serie de ordenadores y un conjunto de dispositivos llamados routers, que son direccionadores o enrutadores que permiten las conexiones entre dos o más redes y seleccionan las rutas por las que envían los paquetes de información. Cabe mencionar que no existe solamente una ruta para transmitir información de un ordenador a otro. La ruta seguida en cada caso depende de elementos circunstanciales, como la densidad del tráfico o como la existencia de averías en alguna red u ordenador intermediarios.

2.3 Los contratos relativos a internet

2.3.1. Introducción de los contratos afines a internet

Los contratos electrónicos, así como los contratos sobre bienes y servicios, servicios informáticos, y en general, las operaciones que se hacen día a día a través de los medios informáticos (en este caso nos referimos a internet) son una realidad que engloba la normatividad tanto contractual como la del ciberespacio. Por lo tanto el alcance de la nueva tecnología nos exige una mejor adecuación de la norma a la vida práctica, por lo que hay que indagar muchísimo más en normas generales de obligaciones[54] y contratos, puesto que entran en juego en la misma generación de éstos y exigen una adaptación del tratamiento jurídico.

Unos de los principales problemas que hay que abordar en estos contratos son:

a) la inmaterialidad del objeto y,
b) la complejidad de las operaciones informáticas.

Además existe la necesidad de afinar conceptos jurídicos, tales como vicios ocultos, la conformidad, el error y una nueva forma de reconsiderar el equilibrio de las partes.

Davara Rodríguez[55] opina que los contratos informáticos tratan de una categoría que aglutina y refiere los acuerdos concluidos sobre bienes y servicios informáticos. De la misma manera define la contratación informática como aquélla "cuyo objeto sea un bien o un servicio informático, o que una de las prestaciones de las partes tenga por objeto ese bien o servicio informático." Así mismo define como contratación electrónica aquella que se realiza mediante la utilización de algún elemento electrónico cuando éste tiene o puede tener una incidencia real y directa sobre la formación de la voluntad, el desarrollo o interpretación futura del acuerdo.

---

[54] *Ibid.* p. 8
[55] DAVARA RODRÍGUEZ, *Op. cit*, pp. 36-37 y 194.

Cuando se hace referencia al contrato informático también hacemos mención a una categoría que engloba contratos heterogéneos, cuyo único rasgo en común radica en su objeto, por lo que no es necesario encontrar una categoría jurídica ahí donde no hay más que un vínculo real entre estos contratos, no poseen por tanto una tipicidad propia.

Un ejemplo de la importancia adquirida por estos contratos electrónicos es el del sector del mercado de valores, con un sistema informatizado de perfección y ejecución de los contratos de compraventa, dicho sistema adquirido gracias a la expansión de internet en estos ámbitos.[56]

2.3.2. La contratación electrónica

Los contratos electrónicos, desde su surgimiento, se fueron encontrando algunas implicaciones que dan pie a cuestionar si estos contratos realmente tienen eficacia jurídica. Una de estas implicaciones la encontramos en el desequilibrio que hay entre las partes, provocado por el mayor y mejor conocimiento de los elementos fundamentales técnicos en cuanto al proveedor, mientras que por el otro lado encontramos a los usuarios, que por lo regular se ven obligados a aceptar las condiciones contractuales impuestas por el proveedor. En razón de sus necesidades de informatización, esto puede hacer muy familiar al contrato de adhesión[57].

M. Jaccard[58] manifiesta que la contratación electrónica presupone la transmisión inmaterial a través de redes informáticas de declaraciones negociables y la marginación de documentos en papel. El objeto de estos contratos puede recaer sobre un bien material cuya entrega física es necesaria para el cumplimiento, pues sólo en algunas ocasiones se trata de prestaciones susceptibles de ser ejecutadas por medio de la transmisión a través de la propia red de información digitalizada. En esta definición podemos observar que trasciende al contrato electrónico generalizado, como un contrato que utiliza la red como un medio para

---

[56] DE MIGUEL ASENSIO, Pedro Alberto, *Op. Cit.* p. 311.
[57] *Ibid*, p. 10
[58] JACCARD, M. *Comerse électronique et droit d' auter sur internet*, vol. 70, 1998, pp. 57-67.

llegar al fin, y que este medio hay que pulirlo para no encontrar lagunas de normatividad que hagan posible la ineficacia del contrato o su incumplimiento.

A) Clasificación de los contratos electrónicos

Es importante dejar explicado que los contratos electrónicos engloban figuras negociables, por lo que tenemos que hacer mención a determinadas categorías de acuerdos que revisten interés, como lo son:

a. Acuerdos de Intercambio Electrónico de Datos.
b. La protección de datos en el ámbito de las comunicaciones electrónicas.
c. Comercio electrónico directo e indirecto.
d. Medios de emisión de las declaraciones de voluntad.
e. Contratos de consumo.

Así mismo, tenemos que tratar la agrupación de los contratos celebrados a través del Internet en función de dos criterios diversos, por una parte que servicios sean utilizados para emitir las declaraciones de voluntad negociables, por otra, el eventual empleo de las redes informáticas en ejecución de las prestaciones.

a. Acuerdos de Intercambio Electrónico de Datos

EDI es el acrónimo de Electronic Data Interchange (Intercambio Electrónico de Datos), su origen se remonta a los años setentas pero es en la década de los ochentas cuando se consolida este sistema de transmisión de datos que puede llegar a servir de medio para la conclusión de contratos o para la comunicación de otras declaraciones de voluntad jurídicamente relevantes.[59]

[59] MEORO CLEMENTE, Mario E y CAVANILLAS MÚGIA, Santiago, *Responsabilidad Civil y Contratos en Internet*, Editorial Comares, Granada 2003, p. 119.

Como lo había comentado con anterioridad, en el campo de la tecnología es muy difícil detectar qué es lo que surge primero, saber si la necesidad origina la solución o si el avance tecnológico se produce previamente y es explotado después para la obtención de utilidades. Esto es lo que pasa con EDI: consiste en la elaboración en el ordenador del emisor, de un mensaje estructurado, es decir, compuesto de unos campos predeterminados y con empleo de una sintaxis y códigos igualmente normalizados; el objetivo de este esfuerzo de codificación y estructuración no es otro que permitir que el mensaje al llegar al receptor sea tratado automatizadamente por las aplicaciones del receptor con ahorro de tiempo, mano de obra y reducción de riesgos y de error en la manipulación de los datos.

A nivel internacional, la Unión Europea y las Naciones Unidas trabajaron mucho en estandarizar la organización y los tipos de mensajes, sus campos y algunos datos codificados, así que la intervención de un sistema como EDI supone la aceptación previa por parte de los participantes de un programa o acuerdo sobre qué mensajes serán objeto de intercambio y con qué contenidos y estándares. Además deben de contar con el programa necesario para traducir los mensajes y normalmente concertar el servicio de comunicación con el líder del grupo o con el tercero que hace las veces de intermediario tecnológico entre todos los miembros. La pregunta es por qué el sistema EDI se encuentra generalizado exclusivamente en grupos cerrados de empresarios que mantienen entre sí relaciones de tracto continuado y de contenido altamente repetitivo; un ejemplo son las empresas de fabricación de componentes ya sea del sector de la automoción o el sector del transporte.

La introducción del Intercambio Electrónico de Datos (EDI), en el que la información transmitida está estructurada conforme a las normas técnicas convenidas como lo veíamos en el párrafo anterior, fomenta la seguridad jurídica al pactar el régimen de cuestiones carentes con frecuencia de regulación en los ordenamientos nacionales, al tiempo que recoge el compromiso de las partes de que el intercambio electrónico de datos

es una vía para la formación entre ellas de contratos con la misma eficacia que los concluidos por medio del intercambio de documentos de papel.[60]

El acuerdo EDI debe diferenciarse de los contratos que se formalicen como consecuencia del intercambio de mensajes de EDI entre los contratantes, ya que estos acuerdos se refieren únicamente a la concertación de las prestaciones.

El contenido esencial del clausulado de estos modelos de acuerdos coincide en la aceptación de EDI como medio de celebración entre las partes de contratos válidos e incluso en la determinación del momento y lugar en que cada uno se considerará celebrado; admisibilidad como prueba, medidas de seguridad, registro y almacenamiento de los mensajes EDI, confidencialidad de los datos, requisitos técnicos para la explotación del EDI, responsabilidad de las partes y de los intermediarios, cláusula de sumisión judicial o arbitral.

En el funcionamiento de EDI la dimensión técnica es imprescindible para hacer posible un formato de mensaje uniforme en el que la información se halla estructurada y que permite que sea procesada por el ordenador receptor[61]. Las especificaciones técnicas se hallan contenidas en un anexo del acuerdo de EDI, siendo frecuente en el entorno europeo el recurso a las normas y recomendaciones UN/EDIFACT, elaboradas por la Comisión Económica para Europa de Naciones Unidas.

b. La protección de datos en el ámbito de las comunicaciones electrónicas

Como ya sabemos, la utilización de las redes de comunicaciones electrónicas puede generar graves riesgos para la intimidad de las personas. Las personas que prestan servicios a través de ellas pueden llegar a conocer un enorme número de datos donde se puede ver claramente sus preferencias y su perfil y cabe la posibilidad de que estos datos sean revelados o sean objeto de comercio con personas interesadas en los datos. Por este motivo, los doctrinistas

[60] HORNING,R.A., *The Enforceability of Contracts Negotiated in Cyberspace,* International journal of law and Information Technoligy, Vol. 5, 1997, pp.109-157.
[61] *Ibidem,*. p.28.

y los legisladores tienen la responsabilidad de custodiar que se cumplan y no se violen los derechos de privacidad, intimidad y confidencialidad de cada persona.

En España existe un Grupo de Trabajo de Protección de Datos, creado por el artículo 29 de la Directiva 95/46/CE, que se ha dedicado a la protección de datos en el ámbito de las telecomunicaciones y en internet; existe otro grupo que está encargado únicamente del cuidado de la protección de datos en el ámbito de las telecomunicaciones denominado Grupo Berlín.

El legislador español propone establecer mecanismos de protecciones adicionales y complementarias a los previstos en las normas generales de protección de datos, mediante la opción de una norma específica. Actualmente la nueva directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas es la Directiva 2002/58/CE del Parlamento Europeo y del Consejo del 12 de julio de 2002, y la anterior la Directiva 97/66/CE, del Parlamento Europeo y del Consejo del 15 de diciembre de 1997.

La Directiva 97/66/CE debe ser adaptada al desarrollo de los mercados y de las tecnologías de los servicios de comunicaciones electrónicas para que el nivel de protección de datos personales y de la intimidad, ofrecidos a los usuarios de los servicios de comunicaciones electrónicas disponibles al público sea el mismo con independencia de las tecnologías utilizadas, es decir lo que pretende España con su nueva directiva es dar el cumplimiento al principio de neutralidad tecnológica, de tal modo que la protección de los derechos de los ciudadanos sea similar con independencia del tipo de comunicación que motive al tratamiento.

Uno de los errores más notables de la anterior directiva está en el apartado 6 de la Exposición de Motivos: "Los servicios de comunicaciones electrónicas disponibles al público a través de internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad" o el apartado 16 de la misma cuyo

alcance se extiende incluso a los servicios de video a la carta, en que la información identificada del usuario ha de considerarse parte de una comunicación.

La nueva directiva regula cuestiones que excedían la anterior directiva tales como la exigencia del consentimiento para el envío de correo electrónico no solicitado (Spam) o la regulación detallada del tratamiento de los datos de localización de terminales de telefonía móvil.

Algunos de los derechos que otorga la nueva directiva a los usuarios son:

I. Que los datos de facturación y tráfico de los usuarios sean eliminados o hechos anónimos cuando no sean necesarios a los efectos de transmisión de una comunicación (artículo 6.1).

II. La conservación de los datos necesarios a efectos de facturación a los usuarios y pago de las interconexiones únicamente hasta la expiación del plazo durante el cual pueda impugnarse la factura o exigirse su pago (artículo 6.2).

III. El proveedor de servicios de comunicaciones electrónicas sólo trata los datos de los usuarios para la promoción de servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido en caso de que el abonado haya prestado su consentimiento, para ello dicho consentimiento es revocable (artículo 6.3).

IV. A no figurar en las guías telefónicas (artículo 12.2).

V. A que sus datos no sean tratados para la prestación de servicios de búsqueda inversa o sin su consentimiento (artículo 12.3).

VI. A no recibir llamadas telefónicas automáticas sin intervención humana, envíos de fax o mensajes de correo electrónico, incluidos los de SMS, con fines de venta directa sin haber otorgado su consentimiento para ello (artículo 13.1).

El legislador español, en lo que al marco regulador de las nuevas tecnologías se refiere, ha reaccionado con rapidez al establecimiento de un nuevo marco normativo comunitario en el ámbito de las comunicaciones electrónicas, por lo que se encuentra en fase muy avanzada de tramitación el Proyecto de la nueva Ley General de Telecomunicaciones. Este proyecto viene a mejorar en gran medida el marco establecido en la actualidad en que las normas de protección de datos, en el ámbito de las telecomunicaciones, aparecen básicamente reguladas en la norma reglamentaria: El Real Decreto 1736/1998, de 31 de julio, de desarrollo del título III de la Ley 11/1998 de 24 de Abril, General de Telecomunicaciones.

El proyecto reconoce el derecho fundamental de los usuarios de los servicios de telecomunicaciones a la protección de sus datos de carácter personal, haciendo expresa referencia a este derecho en su artículo 3, dentro de los objetivos y principios de la Ley. Además, el proyecto introduce la regulación, los derechos de los ciudadanos relacionados con la protección de sus datos personales recogiendo expresamente esos derechos.

Se establece así un marco regulador de la protección de datos en el ámbito de las comunicaciones electrónicas que podrá interpretarse de manera armónica con la legislación general reguladora de tan importante derecho fundamental.

Debe recordarse que además de los derechos mencionados se recogen los derechos ya recogidos por el Real Decreto 1736/1998, los cuales se refieren al tratamiento de datos de localización y el derecho a no recibir llamadas automáticas sin intervención humana, mensajes de fax, mensajes de correo electrónico, o mensajes de datos a terminales fijas o móviles, con fines de venta directa sin haber prestado consentimiento previo o informado para ello.

c. Comercio electrónico directo e indirecto objeto del contrato

El comercio electrónico indirecto comprende las transacciones realizadas por medios electrónicos, relativas a bienes tangibles, es decir un objeto material que existe dentro del mercado pero cuya entrega no puede tener lugar en línea, por lo que la ejecución de esa obligación coincide con la que tendría lugar de haberse concluido la transacción por medio del comercio tradicional. En otras palabras se realiza una compraventa a través de internet y ya sea por medio de mensajería o algún otro tipo de correo, se recibe el bien que uno adquirió al realizar esa compra. En cambio el comercio electrónico directo engloba aquellos contratos electrónicos relativos a la entrega a través de la red de bienes sin soporte físico, o bien información digital. La mayor parte del comercio electrónico directo está constituida por contratos cuyo objeto son bienes protegidos por derechos de propiedad intelectual: obras musicales, imágenes, obras multimedia, bases de datos, susceptibles de transmisión a través de la red. Esto da pie a la explotación de las obras, así como a la piratería. En todo caso tratándose de contratos sobre estos bienes debe dejarse constancia de si pertenecen al suministrador y del alcance de la cesión de derechos. En los contratos sobre bases de datos del suministrador se obliga a permitir el acceso a la información pactada, comprometiéndose a asesorar al usuario sobre el modo de llevar a cabo la obtención de datos[62].

d. Medios de emisión de las declaraciones de voluntad

Como lo habíamos visto con anterioridad, los contratos se forman con el consentimiento de la declaración de la voluntad tanto de una oferta como de una aceptación[63], pero ahora no nos referimos a un contrato que se lleve a cabo de manera tradicional sino a un contrato que tiene diferentes escenarios como internet y que se puede llevar a cabo la declaración de

[62] ALONSO CALERA, GETE, *La contratación en materia Informática*, Editorial La Ley, 1992, pp.1036-1058.
[63] *Ibid*, p. 2.

la voluntad en este margen. Ahora cabe distinguir dos situaciones básicas, por una parte los intercambios de mensajes de correo electrónico que típicamente son mensajes de textos no estructurados, en comparación con los mensajes de EDI, y por otra parte encontramos los contratos propiamente en línea, a través del contrato interactivo con un sitio web, en los que el comportamiento básico del adquirente normalmente es completar un formulario elaborado por el proveedor del contenido. En este caso debe tenerse en cuenta el régimen general sobre información y comunicaciones comerciales.

e. Contratos de consumo

El uso de internet para la comercialización de bienes al público ha permitido el acceso a la contratación electrónica del usuario final que adquiere, a través de la red, bienes o servicios con un propósito ajeno a su actividad profesional. Aquí se convierten en habituales los contratos de consumo transfronterizo, pues el nuevo medio facilita el contacto comercial del consumidor, desde su propio domicilio, con entidades situadas en el extranjero. Actualmente es muy frecuente que un particular situado en México a través de su computadora visite un sitio web de alguna tienda o empresa extranjera, supongamos Estados Unidos, conectado también a través de un servidor norte- americano en la que se ofrecen ciertos productos o servicios para cuya adquisición se requiere al consumidor que responda a una serie de preguntas acerca de sus datos y teclee mostrando su aceptación a los productos o servicios seleccionados y a las condiciones de la operación. En función del carácter inmaterial o no de los bienes solicitados y de la modalidad de pago seleccionada puede ocurrir que todas las obligaciones contractuales deban ejecutarse a través de la red; la cuantía económica de cada transacción es en la mayoría de las ocasiones pagada a través de un intermediario financiero, es decir una tarjeta bancaria lo que ha puesto en relieve que los intermediarios financieros a través de los cuales tienen lugar el pago de los productos y servicios adquiridos en internet pueden ocupar, en la práctica, un papel relevante en la medida en que en determinadas circunstancias pueden controlar el exceso de compras al consumidor. Ya que las operaciones llevadas a cabo para adquirir productos y servicios son, usualmente, poco costosas, apenas resultan operativos los costosos medios

tradicionales de solución de controversias (transfronterizas), justificando el desarrollo progresivo de mecanismos peculiares de mediación y arbitraje en línea.

Los contratos por internet deben de tener un nivel de protección de los consumidores equivalente al que opera en las transacciones tradicionales. Por ejemplo: derecho a recibir información y a que esta información sea fiable y con carácter previo, tutela frente a las prácticas de comercialización no solicitadas y engañosas (ya que esto es indispensable para generar la confianza de los consumidores en el escenario de internet porque el desarrollo del comercio electrónico en internet plantea riesgos para los consumidores), la posibilidad de enviar pedidos simplemente pulsando una tecla y el diseño de páginas web, sin posibilidad de inspeccionar fisicamente los productos, la potencial falta de estabilidad de la contraparte en la medida en que se contrata con su establecimiento virtual y el empleo generalizado de los contratos de adhesión.[64]

Es necesario que las páginas web dedicadas al negocio con consumidores ofrezcan la identificación, localización fisica, vías de contacto por parte del consumidor, números de registro públicos, códigos de conducta o sistemas de certificación en los que participa o mecanismos de solución de controversia sobre las características de los productos y servicios así como las transacciones con información precisa, fácilmente accesible y completa en cada uno de los idiomas empleados incluyendo el costo exacto de los bienes, las condiciones de entrega o puesta a disposición, términos de pago, restricciones geográficas o de tiempo, avisos de seguridad, servicios postventa disponibles, posibilidades de revocación y condiciones de terminación, así como garantías disponibles, todo esto para que el consumidor tenga confianza en la página para realizar la operación y también para que se le permita identificar bien los productos así como a la hora de manifestar su consentimiento pueda obtener un recibo de la operación realizada.

[64] *Ibid.* p. 10.

2.4. Formación de un contrato electrónico

Como lo había señalado con anterioridad la manera típica de llevar a cabo un contrato es con la concurrencia de la oferta y de la aceptación, pero ahora la contratación electrónica va unida al empleo de medios técnicos modernos que están lejos de los medios tradicionales en la emisión de declaraciones de la voluntad.

Ahora el problema con el que nos encontramos es que el legislador acepte el desarrollo de este tipo de contratación o sea que el ordenamiento atribuya a las declaraciones de voluntad negociables expresadas en mensajes de datos transmitidos a través de redes informáticas efectos jurídicos equiparables a los de las declaraciones expresadas por medios tradicionales.

En la normatividad española, a los contratos electrónicos y a los contratos tradicionales los rige el principio de libertad de forma de los contratos y se admite la eficacia obligatoria de las declaraciones emitidas por medios de comunicación que sean producto de la evolución tecnológica como el telégrafo, telefax y correo electrónico. Hay que tener en cuenta que España ya cuenta con una ley aprobada por su congreso en cuanto a firma electrónica y que gracias a esta ley se han derivado muchísimos avances en cuanto a normatividad.

En el ordenamiento español la validez y fuerza obligatoria de un contrato no resulta en principio afectada por la circunstancia de que las declaraciones de voluntad negociables hayan sido emitidas por medio de datos comunicados entre terminales de ordenador; este principio no se impone con certeza en muchos ordenamientos, lo que ha motivado su inclusión como elemento básico en la Ley Modelo de UNCITRAL, cuyo artículo 11 que se vincula con el artículo 5 contiene el principio básico de que los mensajes de datos no deben ser objeto de discriminación respecto de los documentos consignados en papel. Se prevé que, salvo pacto en contrario, la oferta y la aceptación contractuales podrán ser expresadas por medio de un mensaje de datos, al tiempo que establece que no se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un

mensaje de datos, sin perjuicio de que las legislaciones estatales establezcan excepciones en supuestos en los que exijan ciertas formalidades como presupuesto de la válida celebración de un contrato. La concurrencia de la oferta y de la aceptación y la configuración de éstas por medio de internet requiere consideraciones especiales.

La formación del contrato mediante la concurrencia de oferta y aceptación exige una declaración que incorpore todos los elementos esenciales del contrato sin reserva de consentimiento ulterior por parte de quien la formula y otra que acepte la oferta sin modificaciones antes de su caducidad que pueden realizarse con libertad de forma y a través de cualquier medio para su emisión. La valoración de si el contenido de un mensaje de correo electrónico constituye verdadera oferta o aceptación a los efectos de hacer posible la perfección del contrato se plantea típicamente en términos semejantes al empleo de otros medios de comunicación que hacen posible el intercambio a distancia de mensajes de texto; por otra parte la configuración de las declaraciones negociables y la aptitud de éstas para ser consideradas verdadera oferta o aceptación presentan cuestiones peculiares cuando su expresión tiene lugar por medio del contacto interactivo con páginas web.

Muchas de las páginas web que se encuentran en internet no precisan los supuestos constitutivos de verdaderas ofertas frente aquellos que incorporan meras invitaciones a ofrecer, esto es común en las propuestas dirigidas a personas indeterminadas y en las comunicaciones publicitarias. Hay que tener en cuenta la cultura de cada país. En los ordenamientos del common law se sigue una técnica casuística basada en el análisis de los términos empleados y de la naturaleza de la transacción para valorar si concurre la intención de vincularse, mientras que en los sistemas continentales prevalece un análisis centrado en la presencia en la propuesta, aunque dirigida a un número indeterminado de personas, los elementos esenciales del contrato determinante del carácter de oferta vinculante.

A) Los requisitos de forma de un contrato electrónico

Pueden ser exigencias legales que imponen una determinada forma como presupuesto de la válida celebración de un contrato o asocian a la misma cierta eficacia probatoria de la consecuencia de un acuerdo de las partes acerca de la documentación del contrato. En España rige en su ordenamiento el principio de libertad de forma; sólo excepcionalmente se impone una forma determinada como presupuesto de la validez del contrato, por otra parte en determinadas situaciones se exige la formalización por escrito, como sucede con carácter general en los contratos de seguro.

A falta de documentación en papel que acredite la validez en la contratación mediante el intercambio de datos entre terminales informáticos, surge la incertidumbre acerca de en qué circunstancias cabe considerar que estos contratos se han documentado en un escrito, cuál es su valoración como medio de prueba del contrato y en qué medida es posible que satisfaga el requisito de forma escrita cuando éste se impone como presupuesto de la validez del contrato. La Ley Modelo de UNCITRAL adopta el llamado criterio del equivalente funcional, que se basa en la posibilidad de dar cumplimiento a los requisitos legales de forma (sin perjuicio de la posibilidad de dejar al margen ciertos supuestos, como aquéllos en los que se impone la intervención de un fedatario público, excepcionales en el tráfico mobiliario) mediante el empleo de técnicas de comercio electrónico adecuadas para satisfacer los objetivos y funciones a los que responden. Así se refleja en sus artículos del 6 al 8, que determinan las normas básicas que deben cumplir las declaraciones de voluntad negociables para que satisfagan los requisitos de que la información conste por escrito, esté firmado y sea original.

Si bien en un principio un documento electrónico no es legible, como parece característico de los documentos escritos, sí puede transformarse en legible; conforme al artículo 6 de la Ley Modelo, la mera constancia escrita del contrato debe considerarse cumplida cuando la información que contiene es accesible para su ulterior consulta; solución razonable en la medida en que no contempla funciones específicas de un escrito,

ni se le atribuye un especial valor probatorio, sino únicamente se contempla el elemento básico de que la información escrita puede ser reproducida y leída. Cabe considerar que entre los medios de comunicación comprendidos en la expresión por escrito, según el artículo 13 CVIM[65], se encuentran, además del telegrama y telex expresamente mencionados, otros productos del desarrollo tecnológico, de mucha mayor trascendencia práctica en la actualidad y que posibilitan que la información sea accesible para su ulterior consulta, como el correo electrónico. Si bien de lo dispuesto en los artículos 12 y 96 CVIM puede derivarse la necesidad de considerar las soluciones previstas en materia de forma en una legislación nacional, desplazando el principio de libertad de forma.

Si la forma escrita opera como presupuesto de la validez del contrato, se exige no sólo que éste conste por escrito, sino que este escrito además tenga la firma manuscrita de los contratantes, esto se asocia al desempeño de funciones como: identificaciones de los contratantes, certeza de su participación personal, demostración de la aprobación del contenido del documento. El artículo 7 de la Ley Modelo propone métodos que aseguran la posibilidad de satisfacer esas funciones en la contratación electrónica, así como de garantizar la integridad de la información, lo que justifica el reconocimiento por el ordenamiento jurídico de que la presencia de esos métodos en los contratos electrónicos hace posible que estos satisfagan la exigencia de forma escrita y con la firma de los contratantes, junto con la adopción de normas específicas sobre firma electrónica.

B) ¿Cuándo se determina el momento y lugar de celebración de un contrato?

La determinación del momento de celebración del contrato resulta controvertido siempre que las declaraciones de voluntad negociables se intercambian entre ausentes a través de medios que no permiten una comunicación inmediata entre las partes. Nos encontramos ante una dificultad en la contratación entre ausentes. En el Código Civil español y en el Código de Comercio se encuentran unas reglas sobre esta cuestión, que adoptan soluciones diversas, bien conocidas en el panorama comparado, donde el tratamiento varía según los ordenamientos.

---

[65] Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías.

El artículo 1262 del Código Civil español[66] habla de aceptación hecha por carta y establece como momento relevante el de la llegada a conocimiento de quien hizo la oferta, si bien es opinión consolidada que esta norma debe interpretarse en línea con la llamada teoría de la recepción, según la cual el momento de perfección es aquél en que la aceptación llega al entorno del oferente permitiendo a éste tener conocimiento de la misma con una actuación diligente.

El artículo 54 del Código de Comercio español[67] no aplica cuando se trata de contratos con destinatarios finales de los bienes, sin embargo considera que la aceptación se produce desde el momento en que se contesta aceptando la oferta.

En la normatividad internacional, el CVIM[68] en su artículo 15.1 prevé que: "La oferta surtirá efecto cuando llegue al destinatario." El artículo 24 CVIM dice que: "La declaración de aceptación o cualquier otra manifestación de intenciones llega al destinatario cuando se le comunica verbalmente o se entrega por cualquier otro medio al destinatario personalmente, o en su establecimiento o dirección personal".

Por lo tanto se opta por la teoría de la recepción, criterio que también se adopta en los Principios de UNDITROIT[69], en su artículo 1.9 dice: "La comunicación surtirá efectos cuando llegue a la persona a quien vaya dirigida y se considerará que una comunicación llega a la persona cuando le es comunicada oralmente o entregada en su establecimiento o en su dirección postal."

---

hecha en Viena el 11 de abril de 1980 (BOE núm.26, de 30-I-91).

[66] Código Civil, Editorial Aranzadi, Madrid 1993.

[67] Código de Comercio, Editorial Aranzadi, Madrid 2000.

[68] Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías, *Op. cit.*

[69] UNDITROIT, Principios sobre los Contratos Comerciales Internacionales, Roma, 1995.

La UNIDROIT hace un comentario explicativo acerca del momento en el que una comunicación llega a su destinatario. Precisa que "no es necesario que la comunicación en cuestión llegue a manos del destinatario. Es suficiente que sea puesta en manos de un empleado del destinatario que se encuentre autorizado para aceptarla, o que sea depositada en el buzón del destinatario, o sea recibida por su telefax, teléfono u ordenador," así mismo señala que la opción por el principio de recepción encuentra su fundamento en que se considerará más sensato localizar el riesgo de la transmisión en quien escoge el medio de comunicación.

La rapidez en el intercambio electrónico de datos, característica de la tecnología de la sociedad de la información tiende a reducir la importancia de la referida disparidad de soluciones en la medida en que facilita la simultaneidad de las comunicaciones[70], por lo que la determinación de la celebración del contrato se considera contratación entre presentes. La aplicación de las reglas al entorno tecnológico de internet, en el que cabe diferenciar situaciones en las que varía el carácter simultáneo o no de la comunicación de declaraciones negociables, provoca en ocasiones incertidumbre de que sea o no entre presentes.

Cuando la formación del contrato se produce mediante el empleo de servicios interactivos que permiten el intercambio simultáneo de información, situación que normalmente se da en la malla mundial, predomina la idea de que se trata de medios de comunicación a distancia que posibilitan una información instantánea y no sucesiva del contrato, de modo que el tratamiento del momento de celebración debe ser equiparado al de otros medios instantáneos como el teléfono pues permite la comprobación inmediata de que la declaración de voluntad ha sido recibida por el destinatario.

La distinción se difumina como consecuencia del desarrollo de servicios de internet, en particular la mensajería instantánea que hace posible el intercambio instantáneo y personal de mensajes escritos entre integrantes de una lista que se encuentran conectados en

[70] ÁLVAREZ- CIENFUEGOS SUÁREZ, J. M., *Las Obligaciones concertadas por medios informáticos y la documentación electrónica de actos jurídicos*, Editorial, La Ley, 1992, pp. 1012-1028.

un momento determinado. En consecuencia el empleo de este servicio para el intercambio de mensajes de texto parece hacer posible, frente a la regla general en el uso del correo electrónico, la formación instantánea y no sucesiva del contrato.

La Ley Modelo de UNCITRAL[71], aunque no contiene propiamente normas sobre determinación del momento de celebración del contrato, sí incorpora esos criterios en su artículo 15. Según éste, a falta de acuerdo, el momento de expedición de un mensaje de datos es su entrada en un sistema de información que no esté bajo el control de quien envía el mensaje, mientras que el momento de recepción es el de entrada en un sistema de información del destinatario (salvo que habiendo éste designado uno en concreto, se envíe a otro sistema del destinatario, pues entonces el momento relevante es aquél en el que el destinatario recupere el mensaje de datos). Considerando que la entrada en un sistema de información tiene lugar desde el momento en que puede ser procesado en ese sistema; respecto a la efectividad de la oferta, si bien parece razonable que el riesgo derivado del medio de comunicación elegido recaiga fundamentalmente en quien lo selecciona, es decir quien envía el mensaje que da inicio a la comunicación (esto es la oferta), la equiparación del momento de recepción con la entrada en el sistema de información del destinatario es aceptable en la medida en que no menoscaba la posición del destinatario de la oferta.

C) Condiciones generales de la contratación

Lo más usual en la contratación a través de internet el empleo de cláusulas predispuestas por una de las partes con el propósito de que sean incorporadas a múltiples contratos, llamadas condiciones generales de la contratación; en concreto en la contratación interactiva por medio de páginas web, los titulares de éstas suelen establecer un conjunto de cláusulas que unifican los términos en los que contratan con quienes adquieren los productos o servicios comercializados a través de la malla mundial.

El artículo 5.3 LCGC[72] da una disposición relativa a la contratación electrónica así como a la normatividad de desarrollo de esa posición, contenida en el RD 1906/1999[73] El

[71] Ley Modelo sobre Comercio Electrónico. *Op. Cit.* p. 29.

artículo 5.3 establece que: "En los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma."

El RD 1906/1999 regula el deber de información previa. El artículo 2 "la confirmación documental de la contratación efectuada". El artículo 3 "el derecho a la resolución". El artículo 4 "la atribución de la carga de la prueba". Estas disposiciones presentan en gran medida la trasposición a nuestro ordenamiento de normas de la Directiva 97/7/CE relativa a la protección de los consumidores en materia de contratos a distancia.

El ámbito de aplicación del RD 1906/1999 viene fijado en su artículo 1, que incluye dentro del mismo los contratos a distancia celebrados por vía telefónica, electrónica o telemática que contengan condiciones generales de la contratación en los términos de la LCGC. Expresamente se prevé que no será de aplicación a determinadas categorías de contratos: los administrativos, de trabajo, de constitución de sociedades, sobre relaciones familiares, sucesorios y aquellos cuyas condiciones estén específicamente reguladas por disposiciones obligatorias de carácter general, se excluyen también, en línea con lo dispuesto, en el artículo 4.2 LCGC y en el artículo 1.2 de la Directiva 93/13/CEE: "Los contratos relativos a condiciones generales que reflejen las disposiciones o los principios de los convenios internacionales en los que el Reino de España sea parte". En el artículo 1.2 también quedan excluidos, entre otros, los contratos referidos a servicios financieros de inversión, seguro, bancarios, los celebrados mediante máquinas automáticas y los de arrendamiento de bienes inmuebles excepto los de temporada, respecto a todos los contratos excluidos se limita a proclamar el deber de dejar constancia documental, en forma escrita o en registro magnético o informático, el artículo 5.3 LCGC para los contratos excluidos del RD 1906/1999 y no regidos por una normatividad específica, en estas

[72] Ley 7/1996, de 15 de enero, de ordenación del comercio minorista (BOE núm. 89, de 14-IV-98).
[73] RD 1906/1999, de 17 de diciembre, por lo que se regula la contratación telefónica o electrónica con condiciones generales, de la contratación en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril de condiciones generales de la contratación (BOE núm. 313 de 31-XII-99).

circunstancias, parece apropiado concretar su significado básicamente a la luz de lo dispuesto en el artículo 3 del propio RD por ejemplo acerca de la posibilidad de facilitar la justificación en soporte duradero distinto del papel.

CAPÍTULO III
CRIPTOGRAFÍA

SUMARIO.- 3.1 Sistemas criptográficos 3.2 Infraestructuras de claves públicas 3.3 Algoritmos criptográficos 3.4 Criptología y criptoanálisis 3.5 Criptografía

3.1. Sistemas criptográficos

A) Introducción

En este capítulo trato de demostrar la importancia de la escritura criptográfica y la relación que tiene con la firma electrónica, así como sus antecedentes y cómo fue que surgió. Por lo que se hacen los siguientes cuestionamientos ¿Qué es un sistema criptográfico? ¿Para qué sirve?, y ¿cómo se usa?

La palabra criptografía significa *"el estudio de la escritura oculta*" y esto tiene su raíz etimológica en la palabra griega *kryptos* que significa "lo oculto" y *graphos* que significa "escritura"; con el solo significado podemos entender que se trata de algún tipo de escritura que no va a parecernos que tiene algún significado, de hecho la vamos a ver poco coherente a la vista. De tal manera, se tiene que descifrar y es en esto en lo que consiste la criptografía, en que sólo aquellas personas que realmente forman parte de este sistema o grupo, puedan descifrar lo que está escrito.

B) Antecedentes evolutivos de la criptografía

La evolución tecnológica, el uso masivo de computadoras en red, el aumento de redes descentralizadas e interconectadas y el creciente valor de los datos trasmitidos y almacenados en los sistemas conectados a la red, han dado pie a la falta de protección de las informaciones que se puedan estar transmitiendo en la red, especialmente que en las redes abiertas los mensajes de datos sean interceptados y manipulados a conveniencia de las personas que los alteran (los llamados hackers).

La vulnerabilidad de la información es un punto determinante en la importancia de su seguridad y debe de estar encaminada a garantizar su disponibilidad, por ejemplo el acceso legítimo a la información en los términos fijados por el titular. Este sistema de seguridad debe de contener confidencialidad que excluye la puesta a disposición de personas para usos no autorizados e integridad.

El sistema que puede proveernos de más seguridad para pasar información en redes abiertas es el sistema criptográfico, pero la pregunta ahora es: ¿De dónde surge la criptografia?

Desde la época romana[74], Julio César utilizaba una sustitución alfabética simple, cada letra del mensaje era sustituida por la tercera letra siguiente en el alfabeto por ejemplo "hola = jqnc".

En cambio Gabriel de Lavinde, hizo de la criptografia una ciencia más formal cuando públicó el primer manual sobre criptología en 1379.

Samuel Morse, como la mayoría de la gente sabe, desarrolló su Código Morse en 1832, aunque no es precisamente un código como los otros, es una forma de descifrar las letras del alfabeto mediante sonidos largos y cortos.

IBM creó hace años un código denominado "Data Encryption Standard" que de hecho no ha sido roto hasta el dia de hoy. Así mismo existe un sistema denominado TEF (Transferencia Electrónica de datos) que es la manera de llevar a cabo transacciones monetarias, que suponen usualmente pago y que pueden operar o no en tiempo real, todo esto es por medios electrónicos.

Hoy en día el comercio electrónico ha causado un impacto muy profundo a nivel mundial ya que no se esperaba que se avanzara tanto en su utilización. Esta disponibilidad

de sistemas comenzó su auge a principios de la década de 1980 y creó un nuevo entorno donde se podía compartir la información.

En vocabulario más técnico el autor Andrew Nash William Duane[75] nos dice que cuando los puntos de entrada con tecnología de conexiones de acceso telefónico y acopladores acústicos permitieron el acceso a estas redes, se creó la oportunidad para el crecimiento de una nueva industria dedicada a proteger estos puntos de entrada, a medida que se comenzó a interconectar sitios remotos utilizando líneas dedicadas y conectándolas a través de internet, también se creó el potencial para un amplio acceso con toda clase de personajes indeseables.

Andrew Nash [76] da a un ejemplo de cómo en una zona militarizada se crea toda una lengua de estrategias de defensa y se construyen modelos basados en la mentalidad de la fortificación y las defensas del perímetro así como productos de autenticación para identificar a los residentes ante los guardias en las puertas de entrada. Se construyeron zonas desmilitarizadas para distinguir aquellas áreas donde se permitía el acceso externo a computadoras menos sensibles de aquéllas donde se podía combatir a muerte. Se construyeron barreras de seguridad para separar las regiones dentro de las ciudades en red y limitar el daño que los invasores pudieran causar cuando incursionaran en el sistema y quemaran los datos. Se construyeron sistemas para detectar intrusos y trampas.

Ahora ya no existe un perímetro fuertemente custodiado y a cualquier persona se le permite el acceso a sus datos corporativos. Por ejemplo a los socios para compartir estrategia, tecnología y desarrollo de los productos; también a los clientes para acceder a información que permita soluciones en línea, en lugar de usar un asistente y hacer pedidos.

---

[74] BERNAL, Beatriz, y LEDESMA, J. J., *Historia del derecho romano y de los derechos neorromanistas*, Porrúa, México, 1995.
[75] NASH, Andrew, *PKI Infraestructura de Claves Públicas*, Mc G. H, Colombia, 2002, p. 48.
[76] *Ibid.* p. 56.

Aquí surge un problema cuando alguien entrega su centro de datos a compañías que realizan la administración de los recursos a través del país, sin importar la distancia a la que se encuentren. La conectividad y la administración de su red, la suministran proveedores de servicio de aplicación. Lo único que resulta imposible de identificar aquí es dónde se encuentra el problema y en dónde podría encontrarse el perímetro.

En sí, la criptografía es el proceso de transformación de los datos en forma de cifrado y se lleva a cabo a través de algoritmos. La recuperación de los datos en forma legible sólo es posible por medio de un proceso inverso de descifrado, que exige disponer de una clave secreta. Esto fue un avance de vital importancia e innovación en el desarrollo de la criptología.

La criptografía asimétrica o de clave pública permite el intercambio de información cifrada sin necesidad de que los intervinientes compartan una clave secreta común fijada previamente.[77]

En la asimétrica se utilizan pares de claves relacionadas matemáticamente; una pública que puede ser conocida por todos los usuarios y que se emplea para cifrar mensajes y para verificar firmas digitales y otra privada que debe de conocer sólo su titular y que es imprescindible para descifrar mensajes cifrados con la correspondiente clave pública.

La criptografía de clave pública nos sirve solamente para solucionar los problemas que afectan a los documentos electrónicos.

En la legislación mexicana encontramos el fundamento de la criptografía en el artículo 89 del Código de Comercio citando la definición para los Datos de Creación de Firma Electrónica: "..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."

---

[77] ALCOVER, Garau, *La firma electrónica como medio de prueba* (valoración jurídica de los criptosistemas de claves asimétricas)", CDC. Núm.13, 1994, pp. 11-41.

Aunque la ley no especifica qué tipo de criptografía hay que utilizar, el método más seguro es el de la infraestructura PKI, que más adelante explicaré, aunque una vez más nos encontramos ante la disyuntiva de que el legislador no tipifica qué tipo de criptografía utilizar, por lo que se generarían circunstancias de poca credibidilad y seguridad para usar la firma electrónica, ya que muchos de los métodos de encriptación pueden descifrarse fácilmente.

A continuación muestro un ejemplo práctico de la encriptación de una firma digital:

-------BEGIN SIGNATURE------

IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/ZkBfbeNEsbthba4Blrcnjaqbc KgN
+a5kr4537y8RCd+RHm75yYh5xxA1ojELwNhhb7cltrp2V7LlOnAelws4S87UX80
cLBtBcN6AACf11qymC2h+Rb2j5SU+rmXWru+
=QFMx
------END SIGNATURE------

En este ejemplo de la firma digital podemos apreciar claramente cómo la criptografía envuelve en un código difícil de descifrar la firma de una persona cualquiera. A través de este sistema la firma se encuentra segura, y solamente quien tenga la clave pública y la clave privada sabrá exactamente si dicha firma no está alterada y si es de la persona a quien le debe de pertenecer.

Esta firma puede llegar a garantizar, incluso frente a terceros, la autenticidad, integridad, y el no repudio de la información trasmitida en transacciones en la que los intervinientes no se conocen. La firma digital es producto de aplicar una función matemática al documento a firmar cuyo resultado se cifra por medio de la clave privada del firmante y es verificado con la clave pública correspondiente.

De esta manera podemos apreciar cómo la firma digital se basa en la criptografía asimétrica y esta firma la podemos aplicar a un documento no cifrado. Si vemos más allá

nos daremos cuenta que este sistema también es aplicable para la protección de la propiedad intelectual así como para restringir el acceso a terceros contenidos, también los pagos a través de internet se basan en el empleo de la criptografía de la clave pública.

La OCDE[78] menciona principios políticos de cifrado en los estados que formen parte de la misma. Este sistema debe tener desarrollo de sistemas de cifrado que proporcionen confianza a los usuarios, junto con la publicación de los estándares técnicos de los criptosistemas, promoviendo la cooperación internacional en el ámbito técnico, tutela el derecho a la intimidad y protección de datos, posibilidad de imponer el acceso legal, cooperación y coordinación de las políticas estatales.

Ahora bien, para que la criptografía funcione de manera perfecta necesita tener seguridad electrónica, que permita la construcción de una solución para enviar información de negocios y servicios a través de la red. Mencionamos las siguientes características:

1) Identificación: es reconocer a alguien o algo. En el caso de la criptografía es tener una información en particular con una persona que solamente ella pueda reproducir, y en otra forma es capturar la información para la identificación de esta persona y no dejar que nadie más la tenga.

2) La autenticación: es la capacidad de determinar si una persona es autora o no de un documento o de una firma digital y si reconoce el contenido del mismo; por ejemplo firmar un formulario y comparar la firma del solicitante con un registro anterior.
3) Autorización: es lo que está permitido hacer, una vez que en el sistema se identifica y autentica a una persona, se le permite hacer lo que requiera, sin embargo, con algunas limitaciones, ya que se usa en conjunto con un grupo de reglas para determinar si se permite acceder a ciertos datos o funciones dentro de ese sistema. El ejemplo más común que podemos encontrar es la suscripción a un sistema de televisión por cable; sólo vemos los canales por los que pagamos.

[78] OCDE, "Guidelines for Cryptography Policy" pp.1-5.

4) Integridad: es el proceso de garantizar que la información no cambie, ya que cuando nosotros firmamos un documento electrónicamente, no sólo autenticamos el origen del mensaje, sino que también garantizamos que el contenido no sea modificable y tendremos la certeza que le llegará intacto al destinatario.

5) Confidencialidad: se trata de que nadie conozca el mensaje y que sólo las personas autorizadas lo puedan leer, es decir mantener la información inaccesible para otros.

6) Aceptación: se refiere a que los actos de las personas interesadas no se nieguen, sino que se acepten; la forma en que se puede demostrar esto es a través del uso de una firma digital y el reloj fechador digital seguro; así sabremos cuándo se llevó a cabo ese acto con exactitud y quién lo realizó.

La criptografía se configura como un sistema de seguridad básica para el desarrollo del comercio electrónico ya que protege la intimidad de los intervinientes con las características de autenticidad e integridad. Podemos comprender que la criptografía nos ofrece un sistema seguro para poder interactuar dentro de la Web. Pero ¿es segura la criptografía que se utiliza en México para realizar actos de comercio? ¿Qué tipo de criptografía es la que se utiliza?

Por otro lado, es difícil interpretar la voluntad del legislador, respecto a la definición de datos de creación de firma electrónica en el artículo. 89 del Código de Comercio; sin embargo, situándonos en el lugar del legislador, es posible que haya redactado el artículo de esa manera por la creencia de que la tecnología avanza tan rápidamente, que sería ilógico poner una infraestructura tipo PKI si a la vuelta de dos años es obsoleta y se encuentra un mejor tipo de criptografía. Entonces no queda más que optar por cualquier tipo de infraestructura de claves públicas, que sea segura y la que mejor nos convenga.

En España la Directiva del 977667CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, garantiza la confidencialidad de los mensajes electrónicos y la LGT[79] establece que cualquier tipo de información que se transmita por redes de telecomunicaciones podrá ser protegida mediante procedimientos de cifrado.

En la legislación mexicana, el artículo 52 de la Ley de Instituciones de Crédito, [80]párrafo primero, estipula que "las Instituciones de Crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público, mediante el uso de equipos de medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados sobre procedimientos de datos y redes de telecomunicaciones, ya sean privados o públicos..." De aquí la necesidad de que exista la criptografía, por ejemplo en el caso de las tarjetas de crédito y los bancos que prestan asistencia en línea electrónica a través de internet. En el caso de las tarjetas de crédito, cuando las usamos para realizar compras, la criptografía se encarga de proteger la transmisión de la información de las tarjetas de crédito a través de sesiones seguras en la red. Aunque ya están regulados los delitos informáticos en el código penal, el problema de las tarjetas de crédito surge porque sólo se protege la información hasta llegar al comerciante en línea; una vez que el vendedor recibió la información, ésta se queda almacenada en una base de datos que tiene el vendedor, y las bases muchas veces se encuentran conectadas a la red interna del comerciante; el resultado de dicho sistema es que cuando un hacker encuentra la base de datos del comerciante, la copia y hace uso de las tarjetas de crédito y nos encontramos ante la presencia de un delito informático que se encuentra tipificado en el Código Penal Federal,[81] Título Noveno donde se prevé el acceso ilícito a sistemas y equipos informáticos. Los artículos donde se tipifica perfectamente estos delitos son:

---

[79] Ley 11/1998, de 24 de abril, General de Telecomunicaciones (BOE NÚM. 99, de 25-IV-98).
[80] *Ley de Instituciones de Crédito, Legislación de Banca Crédito y Actividades Conexas*, Ediciones Delma.
[81] *Código Penal Federal*, Ediciones Delma, México, 2003.

Artículo 211 bis I.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida con sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.

Artículo 211 bis 4: Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrá de seis meses a cuatro años de prisión y de cien a seiscientos días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días de multa.

Artículo 211 bis 5: Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique o destruya o provoque pérdida de información que contengan se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrá de tres meses a dos años de prisión y de cincuenta a trescientos días de multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Lo que hay que dejar claro es que estos artículos, cuando hablan de "el sistema financiero protegido por algún mecanismo de seguridad" se refieren (en lo que a seguridad se refiere) al sistema de criptografía que es el que se encarga de que los datos no sean descifrados y por lo tanto no estén a la mano de cualquier persona que quiera realizar alguna fechoría.

Antes de las reformas al Código Penal la culpa de esta situación era de los comerciantes, ya que eran los responsables del fraude en línea, y quien terminaba pagando el costo era el consumidor, a esto había que agregarle la pérdida de confianza entre la gente que compraba a través de internet. Hoy en día con los delitos informáticos tipificados en el Código Penal Federal, al que incurra en robarse información de tarjetas de crédito o información financiera se le encuadrará en el tipo penal de delito informático y a esto habría que agregarle si el delito fue de cuello blanco, que significa si una persona se valió de sus conocimientos para llevar a cabo el delito o los realizó sin tener el conocimiento o coadyuvando.

3.2. Infraestructuras de claves públicas

Anteriormente estuve hablando del sistema criptográfico así como de algunas de sus características, pero no especifiqué la manera como opera dentro de las redes más importantes en el mundo.

Quizá no suena común escuchar un cifrado llamado PKI que en la actualidad es la criptografía más utilizada a nivel mundial, ya que la infraestructura de claves públicas constituye el marco de referencia que permite ofrecer servicios de seguridad dentro de la red que se basan en cifrados, como anteriormente ya lo había explicado de manera general. Existen infraestructuras que utilizan un cifrado puramente simétrico que es el de la clave secreta, y que han fracasado por los problemas de manejo que presentan, su ciclo de vida es muy corto ya que los hackers lo han podido descifrar de manera rápida.

Sin embargo el PKI permite crear las entidades y da la confianza que se necesita para llevar a cabo los procesos de identificación y autentificación para administrar el cifrado de clave pública que ofrece una solución infinitamente más escalable que las infraestructuras anteriores de cifrado y seguridad.

La tecnología PKI ha logrado enormes avances durante los últimos años; este sistema ha tenido recomendaciones X.509 de la Unión Internacional de Telecomunicaciones (ITU) y los estándares PKCS de RSA Laboratorios, que es el cuerpo de trabajo más fuerte en la tecnología dentro de internet; otros grupos de la industria y del gobierno han trabajado para definir perfiles y modelos operacionales que se ajusten a lo que necesita el PKI para cubrir las necesidades de sus comunidades en cuanto a seguridad y comercio electrónico.

El PKI es una infraestructura que funciona mejor cuando se ve menos y la gente no sabe tanto de él. El uso de claves públicas y privadas y certificados para firmar correos electrónicos, autenticarse ante sitios Web, validar transacciones y muchas otras funciones, solamente tiene éxito cuando realmente se ocultan por completo las aplicaciones que el PKI utiliza para realizar esas actividades. El Secure Socket Layer, SSL, es donde el PKI ha tenido mucho éxito, porque es casi transparente para el usuario final y la mayor parte de la funcionalidad que se requiere para soportarla se construye de manera directa dentro de los navegadores de la Web.

3.3. Algoritmos criptográficos

Andrew Nash [82] define a los algoritmos como un conjunto de pasos para resolver un problema matemático en los sistemas de las computadoras; los algoritmos se implementan como partes de un programa que se conoce como biblioteca, donde un programa principal realiza la operación matemática sobre algunos conjuntos de datos llamando a las bibliotecas de algoritmos. Algunas partes se pueden implementar en hardware especializado; un ejemplo complejo serían los chips de aceleración de video tridimensionales que se encuentran incorporados en las tarjetas de video de las PC actuales.

Existe otro tipo de algoritmo, llamado algoritmo criptográfico que son las funciones matemáticas que se diseñan para que se puedan llamar con diferentes conjuntos de datos a

[82] NASH, Andrew. *Op. cit.* p. 56.

fin de entrar en funcionamiento. Un ejemplo quizá algo complicado de entender para nosotros, los abogados, es el de un algoritmo cifrado que se puede llamar con los datos de la tarjeta de crédito para codificarlo una vez y para codificar una receta en otro momento.

CSP es un Cryptographic Service Provider, en esencia es una biblioteca de algoritmos criptográficos con algoritmos de cifrado, algoritmos de firmas, etcétera, los cuales se pueden llamar a través de una interfaz claramente definida para realizar una función criptográfica en particular. Los algoritmos criptográficos son complejos y en algunos casos se benefician de un acelerador de hardware para agilizar las operaciones matemáticas, muchos de los servidores web usan una tarjeta aceleradora criptográfica que realiza las matemáticas complejas de los algoritmos criptográficos en hardware especializado de alta velocidad.

1.1. Criptología y criptoanálisis

Para entender mejor a la criptografía debemos de saber que esta materia se divide en dos disciplinas: la criptología y el criptoanálisis.

Los criptólogos son las personas que se encargan de crear a través de bases matemáticas nuevos algoritmos criptográficos; después de generar sus fórmulas las pasan a una comunidad de criptográfos para que las prueben y analicen a fin de encontrar la debilidad del algoritmo; torturan y atacan al diseño, con el único objetivo de descifrar el código. La base para que la criptografía funcione es que siempre se revise y se trate de descifrar con ayuda de la comunidad cripto-analista. Sin embargo hay otros criptólogos que utilizan el sistema llamado *seguridad en la oscuridad*, que funciona desarrollando algoritmos matemáticos pero no lo dan a revisar a la comunidad de criptoanalistas y se queda en secreto. La debilidad de dicho sistema estriba precisamente, en que no ha sido sometido a una revisión y da pie a que alguien pueda descifrarlos.

Un ejemplo claro que menciona Andrew Nash[83] es la importancia de utilizar una buena criptografía. En 1999 un grupo de noruegos que formaba parte del equipo MORE (Masters of Reverse Engineering,) descifró el CSS (Content Scrambling System) que se usó para cifrar los DVD; este algoritmo lo tienen todos los aparatos reproductores de DVD por lo que sería muy complicado volver a cifrar todos los DVD que existen en el mundo. El algoritmo utilizado se creó en el sistema llamado seguridad de la oscuridad y no superó la prueba de los criptoanalistas; esto da pie a que se puedan hacer fraudes y a que haya piratería.

3.5. Criptografía

La criptografía es tan fácil o difícil como se quiera entender ya que se basa en cálculos que pueden ser muy simples o extremadamente difíciles. Como ya lo habíamos comentado, el cifrado RSA que hasta la fecha ha sido difícil de descifrar, se basa en la factorización de dos números primos, mientras que otros tipos de cifrado se basan en problemas matemáticos difíciles y diferentes. Hay dos tipos de criptografía, una simétrica y otra asimétrica; pero quizá se están preguntando por qué a un abogado le interesaría explicar algo que les corresponde saber a los ingenieros; pues esto es muy simple, hay que saber qué tipo de criptografía es la mejor para cifrar contratos, firmas electrónicas, certificados digitales, información confidencial, etcétera. Lo que trato de demostrar es que el legislador se debe de enterar que no estamos hablando de cosas simples; son cosas que quizá en este momento no se ven tan importantes pero que en muy poco tiempo van a rebasar la legislación en los temas de firma electrónica y la criptografía. Aquí la solución más recomendable es que el legislador regule una criptografía segura y confiable, pero sobre todo, que tanto la legislación como la tecnología vayan de la mano. No estoy proponiendo que existan reformas cada año porque la tecnología avanza rápidamente sino que exista un reglamento al artículo 89 del Código de Comercio en cuanto a criptografía.

---

[83] *Idem.*

A) La criptografía simétrica

Esta clase de criptografía es muy antigua. Los egipcios la utilizaron durante toda su existencia; sin embargo, no podemos decir que sea el mejor algoritmo que exista ya que tiene debilidades pero también posee grandes fortalezas, al igual que los algoritmos asimétricos; lo que hay que hacer es combinar los dos tipos para que las debilidades de uno se cubran con el otro tipo de algoritmo.

Para darnos una idea de lo que estamos hablando tenemos que relacionar las claves criptográficas como si fueran llaves físicas; si se tiene la llave correcta se va a abrir la puerta indicada. Cada algoritmo criptográfico necesita una clave, podemos utilizar un algoritmo criptográfico con cualquier clave que tenga la longitud apropiada y el patrón correcto de bits y de esta manera podrá descifrarse un documento cifrado. Los algoritmos criptográficos simétricos toman el texto claro como entrada. Después usando una clave simétrica obtienen una versión cifrada del texto.

En sí, una clave simétrica no es más que un número aleatorio de longitud correcta; un ejemplo claro es si el algoritmo simétrico tiene una longitud de 40 bits, la clave simétrica tendrá que ser de 40 bits de longitud.

Por lo regular hay un grupo de personas que estudian estos algoritmos, y para saber si realmente funcionan y nadie los puede descifrar, dedican mucho tiempo a atacarlo tratando de romper los datos cifrados.

Ahora la pregunta es: ¿cómo funciona la criptografía para cifrar algo? Se utilizan dos claves, la clave secreta y la clave simétrica. La primera se utiliza para encriptar y no se debe revelar a nadie, ésta es la *clave privada*; la otra debe darse a conocer a todo el público y es *la clave pública*.

Al principio de este capítulo abordamos unos conceptos [84] que debería de tener la criptografía; en el siguiente ejemplo de encriptación nos concentraremos, sobre todo, en la autenticidad e integridad.

Cuando un sujeto, en este caso un abogado, encripta el documento con su clave privada, otro sujeto que sería el cliente, lo desencripta con la clave pública del abogado; de esta forma el cliente tiene la certeza de que el abogado lo generó y lo creó ya que es el único poseedor de la clave privada. Existe otra forma de encriptar donde se aplican los términos de confidencialidad y no repudiación o aceptación: una vez que el abogado encriptó el documento con la clave pública, el cliente lo desencripta con su propia clave privada, de esta forma sólo el cliente puede desencriptarlo por ser el único que posee la clave privada.

El proceso de encriptar un texto no es sencillo. Algunos puntos clave, esenciales en la encriptación son:

1) Se utiliza la misma clave para cifrar y descifrar.
2) El cifrado simétrico es rápido.
3) Es seguro.
4) El texto cifrado que resulta de un cifrado simétrico es compacto.
5) Esta criptografía no se ajusta a las firmas digitales o a la aceptación ya que está sujeta a la intercepción.

B) La criptografía asimétrica

En comparación con los algoritmos simétricos ésta utiliza una longitud de clave mayor para lograr el mismo nivel de seguridad que se obtiene en un algoritmo simétrico y utilizando una clave más corta. Existe un algoritmo llamado RSA; es el más exitoso de clave pública y clave privada. Fue inventado por Rivest, Shamir y Adleman, de aquí proviene el nombre de este algoritmo. La patente de este algoritmo expira en el año 2000 y desde entonces se ha

[84] *Ibid.* p. 58.

empezado a incorporar en protocolos como un algoritmo criptográfico asimétrico de carácter obligatorio. Utiliza claves de 1024 bits para individuos y es el más popular y complejo que se encuentre en uso. Otro algoritmo también reconocido, pero que podríamos catalogar en segundo plano, es el ECC.

RSA Laboratories es una organización dentro de RSA Security cuyo objeto, básicamente, es promover el crecimiento general de la industria de la seguridad, incluso si la investigación o los estándares no benefician a RSA Security en sí misma. Gran parte de los estándares importantes, como la serie de estándares PKCs, fueron desarrollados con el auspicio de RSA Laboratories.[85]

C) Claves públicas y claves privadas

Como lo expliqué con anterioridad cuando generamos una clave simétrica escogemos un número aleatorio de una longitud apropiada, y cuando generamos claves asimétricas el proceso es más complejo, puesto que en lugar de usar una sola clave para realizar la codificación y la decodificación, se utilizan dos claves diferentes, una para cifrar y la otra para descifrar, estas dos claves independientes pero matemáticamente relacionadas siempre se generan juntas.

Esto es complejo porque implica una fuente al azar para poder crear las claves asimétricas; hay que recordar que cuando se completa la generación de una clave asimétrica existen dos claves, la pública y la privada. Todo el mundo tiene que conocer la clave pública pero del otro lado debemos de ocultar la clave privada e incluso en muchas ocasiones ni siquiera nosotros sabemos cuál es nuestra clave privada; de lo que sí debemos de estar seguros es de que las claves asimétricas cifran con una clave siempre y descifran con la otra.

[85] RSA Laboratorios, boletín número 13, Abril 2000 "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lenghts".

Existen varios puntos que deben quedar muy claros acerca de la criptografía asimétrica:

1) Siempre que cifremos algo con la clave pública o privada cualquiera de las dos, debemos de descifrar con la otra clave, ya sea la clave privada o pública.

2) El cifrado asimétrico es más seguro.

3) Al momento de codificar no necesitamos enviar la clave, por lo que no tenemos el problema de que nuestra clave pueda ser interceptada.

4) Aquí las claves que se distribuyen son igual al número de gente que utiliza este sistema.

5) No existe una relación previa entre las partes para hacer el intercambio de claves.

6) La criptografía asimétrica sí puede hacer firmas digitales y las acepta.

7) Es lenta esta criptografía y expande el texto cifrado.

Hay que tener en cuenta que incluso cuando un par de claves se han asignado de forma segura a una determinada persona, esto no prueba ni garantiza que esa persona haya firmado, efectivamente, un determinado documento. Aunque en la realidad debería de ser así, que el titular de la clave sea quien firme el documento, pero las firmas digitales permiten que un tercero, autorizado o no, lo firme si está en posesión de la clave privada, lo que podría situarnos en un proceso nuevo de falsificación de firma digital. El titular de una clave privada debe de obligarse a su custodia; su incumplimiento le traería graves consecuencias.

Para la creación de las firmas digitales utilizamos algo parecido a la criptología, son los llamados hashes, unos bloques de datos muy grandes que comprimen los datos

originales como una huella digital. El proceso consiste en tomar un bloque de datos y aplicarle una función matemática; el resultado de dicha operación es el hash que debe de ser un bloque de menor tamaño al original.

La utilización de este sistema de RSA sería lo más adecuado para el comercio electrónico, las firmas digitales y la protección de datos ya que a nivel mundial es uno de los sistemas más eficaces que existen en la actualidad en cuanto a la encriptación de datos.

CAPÍTULO IV
FIRMA ELECTRÓNICA, FIRMA DIGITAL Y CERTIFICADOS DIGITALES

SUMARIO.- 4.1 Firma electrónica 4.2 Certificados digitales 4.3 Extinción del Certificado digital 4.4 Condiciones exigibles a los prestadores de servicios de certificación 4.5 Responsabilidad de los prestadores de servicios de certificación 4.6 Requisitos que deben de cumplir las personas que deseen ser prestadores de servicios de certificación en México 4.7 Eficacia transfronteriza de los certificados.

4.1. Firma electrónica

¿Que es una firma electrónica? ¿Qué diferencia tiene con una firma digital? La Ley Modelo CNUDMI sobre Comercio Electrónico habla de la firma electrónica como un medio para identificar a las personas con las cuales se está interactuando y de esa manera comprobar de qué lugar se adquiere la información y si ésta es fiable para los fines que se creó.

La firma electrónica se creó con el fin de satisfacer exigencias tales como la falta de firma manuscrita a través de los medios electrónicos; ésta en muchos países ha superado la expectativa de una firma electrónica en el ámbito contractual, ya que una de sus características es constituir un signo de identificación personal y representar la voluntad de obligarse.

En la legislación española podemos encontrar que la firma electrónica está regulada en el RDLFE inspirada en la Propuesta Directiva donde se establece un marco común para la firma electrónica[86], este marco común es un riesgo de descoordinación con la armonización comunitaria, ya que Italia y Alemania tenían desde 1997 reglamentos para la firma electrónica.

[86] Propuesta de 13-V-1998-COM (1998)297 final, propuesta modificada de 29-IV-1999-COM (1999) 195 final , a la que se alude en el preámbulo del Real Decreto – Ley 14/1999 y Posición común 28/1999, aprobada por el Consejo el 28 de junio de 1999, con vistas a la adopción de la Directiva, DO 1999 C 243/33.

El RDLF en su artículo segundo define a la firma electrónica "como el conjunto de datos en forma electrónica, anexos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor del documento que la recoge y que si es avanzada permite además detectar cualquier modificación ulterior de los datos a los que se refiere."

Existen diferentes tipos de definiciones en cuanto a firma electrónica. En México, en las reformas al Código de Comercio que salieron publicadas en el Diario Oficial el 29 de agosto del año 2003, el artículo 89 de dicho Código no establece la definición de firma digital, sino que la incorpora como firma electrónica o firma electrónica avanzada; por lo tanto, si se habla de firma digital podremos equipararla a ambas firmas.

La Ley Modelo define a la firma electrónica como "los Datos en forma electrónica consignados en un Mensaje de Datos o adjuntados o lógicamente asociados al mismo por cualquier tecnología que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio."

Si comparamos la definición anterior, con la que da el artículo 89 del Código de Comercio se puede observar que son iguales, ya que estas reformas se basaron en la Ley Modelo.

Podemos darnos cuenta que es diferente la forma en que definen a la firma electrónica en la legislación española pero en esencia es casi lo mismo que las reformas al Código de Comercio y a la Ley Modelo. Quizá ahora queda más claro en qué consiste una firma electrónica: simplemente es un bloque de información que se transmite por internet y que tiene signos distintivos que identifican al destinatario.

¿Qué semejanza tiene la firma digital con la firma electrónica? La firma digital deriva de la firma electrónica, aunque en las reformas al Código de Comercio se consideran iguales. En la doctrina y en el sistema de RSA sí se ve la distinción entre una y otra. Para la creación de la firma digital hacemos uso de la clave privada de quien firma el mensaje de datos, y que a su vez se verifica con la clave pública garantizando la autenticidad del mensaje. Para la creación de esta firma digital se utiliza el hash, en cuanto tenemos nuestro mensaje de datos y ya está firmado; lo que hace el hash es una síntesis del mensaje aplicando un algoritmo que es el que extrae la síntesis, por el cual no se puede recuperar el mensaje original. Hasta que se aplique de nuevo esa función se volverá a obtener el mensaje original, siendo imposible que dos mensajes completamente diferentes puedan dar lugar a una misma síntesis lo que hace que el mensaje sea único; la utilidad que tiene el hash es que cualquier modificación por mínima que sea, al mensaje de texto, en el transcurso de la navegación por internet hasta llegar a su destino, podrá ser detectado por él y esto es lo que le da integridad al mensaje. Los pasos son los siguientes:

1) Se crea el mensaje de datos y se envía con la reseña cifrada; entonces lo que debe hacerse es buscar la clave pública en un directorio.

2) Se utiliza esta clave pública para descifrar la reseña cifrada.

3) Tenemos que tener en mente siempre que la reseña cifrada se creó con la clave privada.

4) La única persona que tiene la clave privada es la que cifró el mensaje.

5) Por lo tanto, si la reseña descifrada y la reseña corresponden, tenemos certeza que está íntegra y que es fiable ya que procede efectivamente del emisor.

La Ley Modelo no regula ni define de forma específica el uso de las firmas digitales, sino que regula de manera general el uso de la firma estableciendo los requisitos de admisibilidad de una firma producida por medios electrónicos y en concreto establece que las funciones tradicionales de una firma son: identificar a una persona, proporcionar certidumbre en cuanto a su participación en el acto llevado a cabo y vincular a la persona con las obligaciones del documento.

La Secretaría General de la CNUDMI está haciendo un estudio sobre las firmas electrónicas y las firmas digitales y se pregunta qué firma sería mejor llevar a cabo, si la de criptografía de clave pública o la asimétrica; ésta última ofrece una manera diferente de la autenticación de firmas manuscritas mediante un dispositivo que se firma en forma manual, utilizando un lápiz especial en una pantalla de ordenador y almacenada como un conjunto de valores numéricos que se podrían agregar a los datos de un mensaje y recuperar en pantalla para que el receptor pudiera autenticar la firma. El sistema permite demostrar la autenticación de un análisis previo de firmas manuscritas y su almacenamiento utilizando el dispositivo biométrico.

La Comisión Europea tiene como principal objetivo desarrollar una política europea sobre la materia, estableciendo un marco común para las firmas digitales; estas medidas al respecto debieron de aplicarse en la Unión Europea antes del año 2000 y por otra parte deben facilitar la confianza en las firmas digitales y ser lo suficientemente flexibles como para admitir los desarrollos tecnológicos. El borrador de propuesta de directiva sobre un marco común para los servicios de firma electrónica presentado por la Comisión Europea mantiene esta distinción y se plantea como objeto alentar dentro de la Unión Europea el uso y el reconocimiento legal de las firmas electrónicas en general y no sólo de las firmas digitales ya que gracias al rápido desarrollo tecnológico se pretende adoptar una posición técnica abierta.[87]

[87] "Communication ensuring security and trust in electronic communication: Towards a European frame work for digital signatures and encryption" de la Comisión Europea (COM (97) 503).

Quizá hasta ahora no comprendamos todavía el significado de una firma electrónica y el de una firma digital; la diferencia es mínima, casi no se puede percibir, sin embargo una firma digital ha sido creada para ofrecer una mayor seguridad que las firmas electrónicas. Las firmas digitales son tecnológicamente específicas, pues como ya lo habíamos dicho, se crean utilizando la criptografía asimétrica o de clave pública y a diferencia de estas las firmas electrónicas son indefinidas por que comprenden cualquier método incluido, pero no limitado al de los sistemas de clave pública.

Una firma digital es una firma electrónica que utiliza una técnica de criptografía asimétrica tal que una persona que disponga de la clave pública del firmante puede determinar si la transformación se realizó utilizando la clave privada del firmante que corresponde a la clave pública del mismo y si el mensaje de datos ha sido alterado; de esta forma, la firma reúne los principios de autenticación e integridad, así como el de confidencialidad.

El Real Decreto Ley Español 14/1999 sobre firma electrónica define: "La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma electrónica el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio valorándose ésta según los criterios de apreciación establecidos en las normas procesales". La misma ley, en el artículo 2, inciso b, define lo que es una firma electrónica avanzada que es lo mismo que las firmas digitales que anteriormente habíamos definido.

El artículo 89 del Código de Comercio[88] en el párrafo octavo y noveno, define a la firma electrónica como "los datos en forma electrónica consignados en un Mensaje de Datos o adjuntados o lógicamente asociados del mismo por cualquier tecnología, que son utilizados para identificar al firmante con relación al mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio."

---

[88] *Código de Comercio. Op. cit.* p. 50.

Este es el fundamento legal en México de que la firma electrónica hace las veces de una firma autógrafa y que es admisible como prueba en juicio. Existe cierta similitud entre la legislación española y la mexicana la diferencia está en que la española no hace tantas distinciones de firma electrónica sino que define una y dependiendo del tipo de criptografía que se utilice, hace la diferencia con las otras firmas.

Una vez que se cuentan con los dos elementos esenciales para crear una firma, el mensaje inicial y la firma hash, debe procederse a la verificación de la firma que consiste en un proceso de comprobación de la firma por referencia al mensaje inicial y a una clave pública dada, determinando de esta manera si la firma digital fue creada para este mismo mensaje utilizando la clave privada que corresponde a la clave pública referida. Dicho proceso tiene dos pasos:

1) Se descifra el hash firmando con la clave privada del emisor y se aplica la clave pública del mismo.

2)..Se aplica la función del hash sobre el mensaje completo que ha obtenido.

Sí el hash que recibido y descifrado coincide con el segundo hash obtenido, significa que en ningún momento hubo algún tipo de falsificación y está íntegra la firma digital del emisor; de otra forma, si uno de los dos hashes ha sido alterado en algún momento, no habrá coincidencia de los dos resúmenes, con lo que el receptor nunca llegará a la misma conclusión.

En resumen, podemos definir la firma digital como la transformación de un mensaje utilizando una función de hash y un criptosistema asimétrico, de forma que una persona que tenga el mensaje inicial y la clave pública del firmante puede determinar de forma segura dos cosas:

a) En el momento que se encripta el mensaje de datos usando la clave privada que corresponde a la clave pública del firmante se satisface la autenticación, porque si el

mensaje se firma con la clave privada de otro sujeto, sólo puede ser verificado por el receptor utilizando la clave pública de ese mismo sujeto.

b) El momento en que se encripta un mensaje de datos se satisface el principio de integridad, aunque tenga una alteración mínima: el resultado de los hashes no va a coincidir con el resumen descifrado y firmado aplicando la clave pública de su emisor, y si el mensaje firmado ha sido alterado no coincidirá con el resumen del mensaje claro.

La firma digital tiene mejores efectos jurídicos en relación a la firma manuscrita, pues cuenta con los principios de integridad, autenticidad y el no rechazo de origen o repudio, por lo que muchas legislaciones equiparan a la firma digital con más o menos exigencias que la firma manuscrita y atribuyendo presunciones a favor de la firma digital.

La propuesta de directiva sobre firma electrónica y servicios relacionados, consideraba que aun así no era 100% segura esta firma, por lo tanto en el artículo tercero, apartado segundo, disponía que los estados miembros "establecerán que los datos sobre los que se ha puesto una firma electrónica y que estén basados en un certificado cualificado válido proporcionado por un proveedor de servicios de certificación acreditado cumplen las exigencias legales de forma y pueden ser utilizadas como medio de prueba ante los tribunales igual que si los datos hubieran existido en forma firmada manualmente."[89]

El Real Decreto Ley español [90] en su artículo 3.1 dispone que los estados miembros asegurarán que las firmas electrónicas que cumplan determinados requisitos de ley satisfacen las exigencias legales de firma manuscrita, y por tanto deben de equipararse a la firma manuscrita en cualquier sentido y en sus múltiples usos, por lo que da pie a preguntarse entonces si es posible hacer un testamento digital, o un testamento ológrafo, ya que para actos tan personalísimos como lo son éstos podría utilizarse una clave privada de firma de considerarse posible y habría de resolverse necesariamente el problema temporal de la determinación fiable y segura del momento de creación de un documento. Estas firmas también son admisibles como medio de prueba en procedimientos legales de la

[89] *Ibidem* p. 59.
[90] Real Decreto Ley. *Op. cit.* p. 64

misma forma que las firmas manuscritas, pero hay que ser objetivos y decir que la admisibilidad como medio de prueba sólo es aceptada en ciertas legislaciones. El derecho español sí lo aprueba como admisible de acuerdo con su Ley de Enjuiciamiento Civil; un ejemplo de ello es la presentación de un documento electrónico firmado digitalmente como medio de prueba de la celebración de un contrato o de la existencia de una declaración por medios electrónicos.

Los requisitos que deben cumplir estas firmas en la legislación española para que puedan ser aceptas como medio de prueba son:

a) Firmas electrónicas avanzadas,
b) basadas en un certificado reconocido y
c) creadas por un dispositivo seguro de creación de firmas.

Estas exigencias pueden negar la eficacia legal a firmas electrónicas en las que falte algún requisito, por ejemplo el de Certificado Reconocido, y podría suceder que las partes se conocieran perfectamente, intercambiaran manualmente sus claves y acordaran que las firmas digitales creadas serían vinculadas para las partes; no tendría esto validez ya que no existe el certificado de reconocimiento de la firma y por lo tanto no podría ser válido dentro de un juicio, sin embargo, en este ejemplo no se llevó a cabo ningún tipo de fraude o falsificación porque las partes actuaron de manera verosímil, aun así no sería válido.

El mismo Decreto Español en el artículo 5, apartado 2, establece:

> Que los Estados miembros velarán porque no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por:
>
> a) El mero hecho de que ésta se presente en forma electrónica.
> b) No se base en un certificado reconocido.
> c) No se base en un certificado expedido por un proveedor de servicios de certificación acreditado.
> d) No esté creada por un dispositivo seguro de creación de firma.

Los españoles nombran a esta cláusula como cláusula de salvaguarda, ya que si a estas firmas electrónicas no se les podía negar la eficacia, entonces la tenían aunque no cumplieran con todos los requisitos. Lo que nos trata de decir esta cláusula es que se beneficiarán a las firmas electrónicas que cumpliesen determinados requisitos (antes mencionados) con determinadas presunciones que no beneficiarían al resto de firmas electrónicas, y no por eso perderían la validez y eficacia.

Hay que tener en cuenta que esas presunciones legales y normas de atribución serán ciertas siempre y cuando tengan un fundamento técnico adecuado.

En México el artículo 89 del Código de Comercio, continúa poniendo las bases para el proceso de la firma electrónica que en el próximo capítulo veremos detenidamente. Este artículo define los mensajes de datos como "la información generada, enviada, recibida o archivada por medios electrónicos ópticos o cualquier otra tecnología" y el artículo 89 bis de la misma ley: "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". A diferencia de la legislación española, aquí el juez es el que tiene que dar toda la validez como prueba de lo que contenga escrito el mensaje de datos, pero la ley cuando define la firma electrónica dice que si está en un mensaje de datos también será admisible como prueba dentro de juicio. Ahora la pregunta es si esta firma es válida dentro de juicio; ¿necesita ratificarse ante notario? o ¿sólo con la validez que le da la ley es suficiente? El Código de Comercio, en el artículo 100, dice que los certificados electrónicos expedidos no llevan fe pública, sin embargo, faculta a los notarios y corredores públicos a que puedan expedir certificados que impliquen fe pública. Pero el estado le otorga al notario precisamente la delegación de la fe pública, de otra forma no considero prudente que un prestador de servicios sea un notario si no está realizando la función pública investida por aquél a través del titular del Poder Ejecutivo de dar fe para hacer constar actos.[91]

[91] *Ley del Notariado para el Estado de Jalisco*. Artículo 1, *Op. cit.* p. 24.

Sí se comparan las legislaciones en materia de firmas electrónicas el artículo 17 del Reglamento Alemán de firma digital establece que la autoridad publicará en la Gaceta Federal una relación de los algoritmos y los parámetros aplicables que consideren adecuados para la creación y verificación de firmas digitales, así como el periodo para el que dicha adecuación existe en cada caso, el cual debe de ser por lo menos 6 años después de su evolución y publicación y se reevalúa anualmente. Se concluye que existe la adecuación si dentro de un determinado periodo de tiempo la falsificación imperceptible de firmas digitales puede excluirse con absoluta seguridad bajo el estado de la ciencia y de la técnica. La adecuación se determina tomando la base de datos de la oficina federal para la seguridad en tecnologías de la información.

En el presente trabajo hemos estudiado varios conceptos; quizá hasta ahora no hemos entendido, ni las criptografías, ni las claves públicas y peor aún, ni siquiera creemos que puedan ser 100% seguras. Lo repetimos: sí son seguras porque no sólo interactúan un cifrado y unas claves sino también una tercera persona que es de confianza y que se encarga de dar fe que no ha habido falsificación alguna y de que no la habrá a menos que se descifre la fórmula matemática del algoritmo que se esté utilizando para encriptar.

Tercera parte de confianza

La solución a los problemas de falsificación y no reconocimiento, de la firma digital y de la criptografía, es una tercera parte de confianza, la cual actuará para asegurar el vínculo entre la clave pública y el titular de la clave privada; además desempeña otras funciones, como autenticar fechas y horas de las transacciones, publicar electrónicamente las claves privadas que no pueden ser de confianza, en caso de revocación o suspensión, así como adscribir una responsabilidad apropiada para los implicados en el comercio, cuando una de las partes niegue responsabilidad por la transacción. De este párrafo podemos ver cómo surge la intervención del notario en el artículo 115 de la Ley del Notariado para el Estado de Jalisco.[92] Nos da la pauta de que las certificaciones sobre autenticidad de firmas se hará constar en acta que se alcance de los mismos documentos; aquí el notario trabaja como una

[92] *Idem.*

persona que es una tercera parte de confianza o un prestador de servicios de certificación, siempre y cuando lleve esta ratificación o certificación la fecha en que se lleve a cabo, la hora de la firma , los nombres de los comparecientes, sus generales cuando no obren en el documento y la personería cuando actúen a nombre de un tercero.

El artículo 100 del Código de Comercio es el fundamento legal que autoriza al notario y al corredor público a actuar como prestadores de servicios de certificación, sin embargo faculta a otras instituciones públicas y a personas morales de carácter privado. Reiterando el comentario de párrafos anteriores, considero que la ley únicamente debió haber facultado únicamente a los notarios, corredores públicos y las instituciones públicas, ya que los actos que éstos realizan están investidos de fe pública, y también para dar más seguridad, credibilidad y autenticidad a los certificados.

De otra manera podemos decir que la función de una tercera parte de confianza es garantizar la asociación entre un par de claves y una persona determinada; así mismo se encarga de distribuir de manera efectiva las claves públicas. El certificado de un prestador de servicios de certificación relaciona una clave pública con una persona en particular, de esta última precisa su identidad y asegura que es el titular de la clave privada. Cuando se expide un certificado es firmado por el prestador con su correspondiente clave privada para garantizar frente a terceros su integridad y origen.

En la legislación mexicana, el Código de Comercio en el artículo 101 señala cuáles son las actividades que deben de realizar los prestadores de servicios:

> 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 del Firmante y del que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Avanzadas y emitir el certificado.

IV.- Cualquier Otra actividad no compatible con las anteriores.

El notario en el punto primero del artículo anterior, identifica al usuario por medio de documentos de identificación oficial como la credencial del IFE y si esto no es suficiente a través de dos testigos según el artículo 90 de la Ley del Notariado [93]

En el punto segundo, cuando se habla de verificar la firma electrónica se está haciendo referencia a una firma electrónica avanzada fiable, que contenga los requisitos de creación de firma que correspondan exclusivamente al firmante, que los datos de creación de firma estaban en el momento de la firma bajo el control exclusivo del firmante, que sea posible detectar cualquier alteración de la firma electrónica después del momento de la firma. Si llegara a haber alguna alteración a la firma se detecta rápidamente porque se descubre el algoritmo matemático de la criptografía que se utiliza según lo establece el artículo 97 del Código de Comercio. Si la firma contiene estos requisitos podrá tener validez probatoria en juicio, si le faltara alguno no se considerará firma electrónica avanzada o fiable sino únicamente el género de firma electrónica.

Después de haber visto los requisitos de las firmas electrónicas avanzadas o fiables y de los prestadores de servicios podemos concluir que los notarios una vez que hayan realizado la expedición de un certificado electrónico tendrán que asentar los hechos en un libro de registro de certificaciones, y en su respectivo protocolo, pero aquí surge la controversia, ya que estamos hablando de un certificado electrónico, no de un certificado manuscrito, o escrito de puño y letra, sino electrónicamente, entonces el notario debería de tener un protocolo electrónico, para dejar asentado los actos o hechos realizados por éste. Sin embargo, la Ley del Notariado para el Estado de Jalisco no habla de un protocolo electrónico, mucho menos de un programa de captura del notario donde pueda asentar este tipo de actos; lo que sí dice la ley es que si no se inscribe el acto en el protocolo producirá la nulidad y responderá el notario por los daños y perjuicios que se causen, esto según los artículos 87, 116, 117 y 118 de la Ley del Notariado para el Estado de Jalisco[94]. Considero que esto no es justo para los notarios, porque no son los únicos prestadores de servicios;

[93] *Idem.*

también están las personas morales de carácter privado y éstas no tienen protocolo para inscribir este tipo de actos, ni se rigen por una ley notarial.

A nivel internacional, la UNCITRAL prevé para su próximo periodo de sesiones, además de la función de emisión de certificados de clave pública una entidad certificadora como servicios de registro, sellado temporal de datos y comunicaciones basadas en firmas digitales.

4.2. Certificados digitales

Los certificados digitales también son conocidos como autoridades de certificación; usualmente colaboran extendiendo un certificado de una firma digital verificada, garantizando que la clave pública particular esté asociada con equis usuario en particular; ésta es la forma más simple en que podemos explicarnos. Presentan en lista quién es el propietario de la clave pública y contienen una copia de la clave pública de ese usuario, entonces una autoridad de confianza firma la certificación.

En México para que se considere válido un certificado, necesita contener los siguientes requisitos, según el artículo 108 del Código de Comercio:

> 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 la hora de emisión, suspensión y renovación del certificado;
> VII.- El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación;

[94] *Idem.*

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

Una vez que certificamos la firma se crea un hash para todo el certificado y este hash queda codificado utilizando la clave privada de la autoridad de confianza.

Ahora bien ¿cómo podemos verificar la validez de un certificado digital? Lo único que se necesita es usar la clave pública de la autoridad de confianza y si es correcta la verificación podemos estar seguros que la clave privada que está en el certificado pertenece a la persona que lo emite.

Para entender mejor las cosas, la autoridad de confianza crea un certificado con su propia información de identidad, lo mismo que la clave pública de dicha autoridad y la firmará; este certificado se llama certificado autofirmado.

Los certificados usualmente son de información pública y puede darse el caso de que existan muchas copias del certificado publicadas, dado que todo el mundo las puede ver, por lo que cualquier intento de fraude con el mismo certificado será detectado al momento de llevarlo a cabo, ya que uno de los software que usa el certificado siempre realiza la verificación de la firma y si ha sido modificada los valores hash no corresponderán. En este punto, el software rehusará usar la clave pública en el certificado y lo marcará como error.

La manera en que se puede dar a conocer la clave pública es manualmente, ya sea un intercambio plasmado en una hoja o a través de un disquete; nada más que si lo hacemos por este sistema tenemos que imprimirlo antes para cerciorarnos que la clave que se nos está proporcionando es la correcta y que no está modificada.

Hay que aclarar que el sistema de intercambio manual de claves sólo se puede dar con personas de extrema confianza y que se comunican mediante sistemas cerrados, siempre y cuando sea un círculo pequeño de personas ya que si es muy grande se pierde el control de todo.

Lo que trato de explicar con este sistema es que de nada sirve que exista una autoridad certificadora si ésta puede certificar una clave que está falsificada porque la original también lo está; entonces el problema de la certificación no sería de la autoridad sino de las partes que interactúan en las firmas, de ahí que se pueden dar las siguientes hipótesis:

a) Un impostor se hace pasar por el titular y sustituye las verdaderas claves públicas.

b) El emisor comunica al receptor su clave pública que está sustituida por la clave de un tercero, que ahora podrá firmar con la clave privada correspondiente; el receptor creerá que los mensajes son del emisor.

c) La firma digital es falsificada y el mensaje descifrado puede ser revelado a personas no queridas.

Éstas son algunas de las formas posibles en que se pudiera falsificar una firma:

1) El supuesto en que B dice ser A porque en un momento determinado sustituye la clave pública de A por la suya propia; aquí el ladrón logró su objetivo porque se planteó un problema de distribución fiable de la clave pública.

2) El supuesto en que B roba la clave privada de A, por la mala custodia y pérdida del control de la clave pública.

En sí la utilidad de la firma digital como medio de autenticación está condicionada a la posibilidad del receptor de tener garantía de la autenticidad de la clave usada para verificar la firma, ya que una firma digital verificada con una clave pública únicamente garantiza que el mensaje ha sido firmado por el poseedor de la correspondiente clave privada, pero de ninguna manera garantiza la identidad del poseedor de la clave privada y aquí es donde se dan todos lo problemas y surgen las hipótesis antes mencionadas, ya que puede ser un poseedor ilegítimo o un impostor. Esto nos induce a pensar que las firmas manuscritas tienen una asociación intrínseca con una persona determinada porque están

hechas con la misma escritura manual del firmante, por lo que muchos legisladores opinan que un juego de claves (criptografía) no tiene una intrínseca asociación con nadie, ya que un bit es lo mismo que otro bit y estos los poseen indeterminado número de personas que utilizan la criptografía, por lo que muchos legisladores no consideran la relación ya que son simples números.

A consecuencia de los ultrajes que pueden llevarse a cabo con las firmas electrónicas debemos estar concientes de que necesitamos una forma más segura y convincente de asociar una determinada persona o entidad al par de claves. En el comercio electrónico se puede usar este sistema en transacciones importantes entre personas extrañas que no tienen relación contractual previa y quizá nunca vuelvan a contratar una con la otra.

Se plantean varios puntos que pueden contrarrestar la distribución de claves públicas:

1) Registro de claves públicas. Este sistema es muy parecido al que se explicó en la página anterior ya que cualquier persona puede tener acceso a un directorio donde se publiquen todas las claves por lo que este sistema no es el más eficaz.

2) Web of trust. [95] Funciona cuando el receptor del mensaje recibe la clave pública del emisor junto con el mensaje y entonces puede transformarlo y descifrarlo. El receptor debe verificar si la clave pública usada está actualmente asociada con la persona identificada como emisor con otra persona de confianza; esta tercera persona puede decir que conoce y confía en el emisor y su clave pública, añadiendo medidas de confianza en el proceso. La ventaja del sistema es su independencia de cualquier autoridad central; la desventaja es que si el emisor no conoce a alguien de confianza que tenga relaciones con el receptor, tendrá que confiar en un desconocido y así no podrá comunicarse de forma segura con casi nadie.

[95] Es la base del programa PGP (Pret good privacy) encryption system de Zimmerman.

3) Terceras partes de confianza (TTP). [96] Son las autoridades de certificación y certificados. Se considera que es el sistema más adecuado, ya que consiste en la intervención de una o más terceras partes de confianza que emiten certificados. Éstos a su vez sirven para distribuir la clave pública para asociar de forma segura la identidad de una persona con su clave determinada. Aquí en México son mejor conocidos como prestadores de servicios de certificación.

En conclusión, un certificado digital 100% seguro tiene que unir un par de claves con la firma de algún suscriptor o emisor y asociar la identidad de una persona determinada a una clave pública en concreto. Después, el destinatario de un certificado que desee apoyarse en una firma digital creada por el suscriptor mencionado en el certificado, puede usar la clave pública incluida en el certificado para verificar que la firma digital fue creada con la correspondiente clave privada. Si la verificación realizada a través de un certificado es satisfactoria, se obtiene la seguridad de que la correspondiente clave privada es poseída por el emisor o suscriptor mencionado en el certificado y que la firma fue creada por él.

Una vez que una firma digital verificada utiliza un certificado de autoridad, puede proporcionar elementos de mayor valor a efecto de que sea mayor la valoración probatoria de la misma que permite atribuir un mensaje electrónico a una persona en particular, por ello se considera que una firma digital obliga mucho más que una de base de distribución manual de clave pública como lo habíamos mencionado antes.

En países miembros de la comunidad europea existen autoridades de certificación que cuentan con licencia para emitir el certificado por lo que ordenamientos jurídicos establecen una presunción legal *iuris tantum* de que el mensaje electrónico pertenece al titular de la clave. Claro que juridicamente todo se puede desvirtuar, sin que esto pueda afectar al resto de las firmas digitales.

---

[96] TTP Trusted third party es cualquier parte de confianza interviniente en una transacción para prestar servicios de seguridad, la tercera persona que desempeña de forma fundamental la función de emisión de certificados se conoce entre otros, como autoridad de certificación, entidad de certificación proveedor de servicios de certificación o simplemente certificador.

Una clave pública certificada entonces puede utilizarse como una firma digital y puede llegar a utilizarse como un certificado que mejora la fiabilidad del mensaje electrónico

La UNCITRAL[97] tiene una clasificación de categorías de firmas y encabezan la lista las que tienen mejor seguridad jurídica:

a) Firmas electrónicas.
b) Firmas digitales.
c) Firmas digitales certificadas.
d) Firmas digitales certificadas por una entidad certificadora.

En esta lista también entran las firmas digitales certificadas o autenticadas por un notario público o sea aquellas firmas en el que se le pone la firma sobre el mensaje electrónico en presencia de un fedatario público o funcionario especialmente calificado.

Este concepto de la firma digital certificada por un notario público es quizá uno de los conceptos menos estudiados en cuanto a materia de firmas digitales, sin embargo algunas legislaciones no la han pasado por apercibida; una de ellas es Italia ya que el artículo 16 del Reglamento de Firma Digital señala: "La autenticación consiste en la declaración por parte del oficial público de que la firma digital se ha realizado en su presencia por el titular, previa comprobación de su identidad personal, de la validez de su clave pública y del hecho de que el documento firmado corresponde a la voluntad de la parte y no es contrario al ordenamiento jurídico."

En las comunidades europeas, el RDLFE tiene una regulación especial respecto a los certificados digitales. En el artículo 4.1 menciona la adopción de prescripciones específicas para el empleo de la firma electrónica por las administraciones públicas. El artículo 5 del mismo reglamento dice que los prestadores de servicios de certificación

[97] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Informe del Grupo de Trabajo sobre Comercio Electrónico de su labor del 31° periodo de sesiones, A/CN.9/437, del 12 de marzo de 1997, párrafos del 40 al 43.

tienen que hacer posible la obtención de la acreditación de su actividad o la certificación del producto de firma electrónica siempre y cuando haya un organismo encargado de su supervisión.

Los prestadores de los servicios de certificación deben tener un registro dependiente del Ministerio de Justicia de la Unión Europea, en el que deberán de solicitar su inscripción, con carácter previo al inicio de su actividad.

El artículo 81 de la ley 66/1997 del 30 de diciembre[98], sobre medidas fiscales, administrativas y del orden social, dio facultades a la Fábrica Nacional de Monedas y Timbre (FNMT) para prestar en el ámbito de materia de firma electrónica e internet todo lo relativo a los servicios que sean necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos.

El desarrollo de esta norma tiene lugar a través del RD 1290/1999 del 23 de julio que se enfoca en la firma electrónica, por lo que el FNMT junto con correos y telégrafos son los que permiten acreditar la identidad del emisor y del receptor y la autenticidad de su voluntad, garantizar la integridad del contenido del documento y acreditar la presencia o la recepción por el destinatario de notificaciones, comunicaciones o documentación.

En España el órgano competente para acreditar a los prestadores y certificar los productos es la Secretaría General de Comunicaciones, es por esta razón que el otorgamiento de la acreditación o del certificado de conformidad tiene lugar previa evaluación del prestador de servicios o del producto por una entidad de evaluación independiente acreditada por la Entidad Nacional de Acreditación u otra aceptada en la Unión Europea.[99]

---

[98] BOE núm. 190, de 10-VIII-1999

[99] BOE núm. 45, de 22-II-2000.

Los dispositivos seguros de creación de firma son los datos de generación de la firma y que ésta no pueda ser falsificada con la tecnología existente, posibilidad de protección fiable de los datos de creación de firma por parte del signatario contra la utilización por terceros. Si se cumplen estas exigencias, la no alteración de los datos se subordina a la certificación de los dispositivos seguros de creación de firma.

Los efectos jurídicos de la firma electrónica se subordina a:

a) Que se base en un Certificado Reconocido.
b) Que haya sido producida por un dispositivo seguro de creación de firma.
c) Que el certificado haya sido expedido por un prestador de servicios de certificación acreditado.
d) Que el dispositivo de creación de firma se encuentre certificado.

Los certificados reconocidos deben de contener: indicación de que se expiden como tales; código identificación único del certificado; datos de identificación y firma electrónica avanzada del prestador de servicios de certificación que lo expide; identificación del signatario; datos de verificación de firma digitales y si existe algún tipo de representación, ésta debe de constar en el certificado.

4.3. Extinción del certificado digital

Los certificados se pueden extinguir bajo los supuestos del artículo 9 del RDLFE, cuando expire el periodo de validez del certificado, que es de cuatro años, revocación por el signatario o su representado, pérdida o inutilización del soporte del certificado, utilización indebida por un tercero, orden contenida en resolución judicial o administrativa, fallecimiento o incapacidad del signatario o de su representado, extinción de esto, terminación de la representación, cese de actividad del prestador de servicios, e inexactitudes graves en los datos aportados por el signatario para obtener el certificado. En

México no existe mucha diferencia, solamente que el periodo de validez es de dos años en lugar de cuatro, también contempla la extinción del certificado por revocación por el prestador de servicios a petición del firmante y aquí la diferencia más clara es a la hora de la expedición el certificado si no cumplió con los requisitos; es quizá la única diferencia que existe con respecto al reglamento de España en cuanto a la extinción de los certificados.

4.4. Condiciones exigibles a los prestadores de servicios de certificación en España

Los prestadores de servicios tienen que cumplir con ciertas condiciones que plantea el anexo II de la directiva de 1999/ 93 /CE y que son:

a) Comprobar la identidad y circunstancias personales de los solicitantes de los certificados.

b) Poner a disposición del signatario los dispositivos de creación y verificación de la firma y no almacenar los datos de creación de firma salvo que el signatario lo solicite.

c) Informar al solicitante, con carácter previo, de extremos como el precio de sus servicios y las condiciones de uso del certificado.

d) Mantener un registro de certificados en el que consten los emitidos y los datos sobre su vigencia.

e) Comunicar a los titulares de certificados con una antelación mínima de dos meses el cese de su actividad como prestador de servicios.

f) Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.

Si los prestadores de servicios de certificación incumplen estas condiciones se les aplica una infracción administrativa con un específico régimen sancionador.

Los prestadores de servicios de certificación no deben olvidar poner en el certificado la fecha y hora de expedición y extinción del certificado -el RDLFE no exige el empleo de sellos temporales de la firma de los mensajes-, para poder demostrar la fiabilidad de sus servicios y garantizar la rapidez y seguridad del servicio. Además el RDLFE en los artículos 17 y 25 del reglamento del 21 de febrero del año 2000 crea medidas contra la falsificación de certificados y así mismo garantiza la confidencialidad de los datos de creación de firma y la responsabilidad frente a los usuarios de servicios y terceros.

Esta garantía debe de cubrir al menos 6.010.121,04 euros o 4% de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita un prestador de servicios.

El prestador de servicio tiene que conservar durante 15 años toda la información relativa a un certificado reconocido, informar de los criterios que se comprometen a seguir en el ejercicio de su actividad y a los solicitantes, con carácter previo del precio y las condiciones de utilización del certificado.

4. 5. Responsabilidad de los prestadores de servicios de certificación

El artículo 14 del RDLFE fija las normas generales sobre la culpa de los prestadores ya sea contractual o extracontractual; el criterio que sigue este artículo, básicamente, es el de que la responsabilidad que deben afrontar los prestadores de servicios es por daños y perjuicios causados a cualquier persona en el ejercicio de su actividad, se deberá de demostrar que el prestador de servicios no actuó con la debida diligencia, por lo que para que este sistema de certificados funcione bastaría con que se insertara un sistema basado sólo en la culpa, para que el modelo de responsabilidad objetiva con límites fijados en el certificado fuera suficiente para favorecer el desarrollo de las actividades de certificación y de esta manera

proporcionara una mayor protección del tráfico.[100] En la legislación mexicana las responsabilidades de los prestadores de servicios de certificación se estipularán en los contratos que se realicen con los firmantes, pero si el prestador de servicios incumple con las obligaciones que se estipulan en el artículo 104 del Código de Comercio entonces la Secretaría de Economía se verá en la necesidad de sancionar al prestador de servicios, previa garantía de audiencia, con suspensión temporal y definitiva de sus funciones; la materia competente es la Ley Federal de Procedimiento Administrativo, y el artículo 1100 del Código de Comercio.

El prestador de servicios en España solamente será responsable de los daños y perjuicios cuando en el certificado no se haya consignado de forma clara, reconocible por terceros, el límite a su posible uso y lo más importante que es el importe máximo de las transacciones.

4.6. Requisitos que deben cumplir las personas interesadas en ser Prestadores de Servicios de Certificación en México

Actualmente la legislación mexicana en materia de Prestadores de Servicios de Certificación está regulada en el Código de Comercio, capítulo, III denominado "De los Prestadores de Servicios de Certificación."Estas reformas son del 29 de agosto del año 2003 en materia de firma electrónica, publicadas en el Diario Oficial de la Federación. Muy recientemente se publicaron en dicho Diario el 19 de julio del año 2004, el Reglamento al Código de Comercio en Materia de Prestadores de Servicios de Certificación; así mismo en agosto del año 2004 se publicaron las Reglas Generales a las que deberán sujetarse los prestadores de servicios de certificación.

Considero que el Código de Comercio regula de una manera muy ligera la materia de los Prestadores de Servicios de Certificación; el Reglamento del Código de Comercio toca la misma materia de una forma más concreta ya que son normas reglamentarias a las

[100] El Real Decreto Ley sobre la Firma Electrónica, RCE, núm 1,200, pp. 7-27.

que deben de sujetarse los prestadores de servicios de certificación. En cambio las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación publicadas en agosto del 2004, son reglas muy específicas y mucho más concretas ya que hace una descripción detallada de los elementos humanos, elementos materiales y sus procedimientos, elementos económicos, elementos tecnológicos y sus procedimientos, evaluación y análisis de riesgos y amenazas, infraestructura informática, plan de continuidad del negocio, plan de seguridad de sistemas, estructura de los certificados, de la fianza, etcétera. Todos estos temas respecto de los prestadores de servicios, son puntos que también se conceptualizan en el Código de Comercio y en el Reglamento no se describen con la profundidad como lo hacen las Reglas Generales...

El artículo 102 del Código de Comercio, dice:

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 del artículo 100 del Código de Comercio puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaria, la cuál 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 cumplimiento 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. (Estos elementos se encuentran claramente definidos en el Reglamento del Código de Comercio y en las Reglas generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación);

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;

Esta fianza al Notario que desee prestar y aplique para ofrecer sus servicios como prestador de servicios de certificación se le pide una fianza de cinco mil veces el salario mínimo general diario vigente del Distrito Federal.

VI.- Establecer por escrito su inconformidad para ser sujeto a Auditoría por parte de la Secretaría, y

VII.- Registrar su Certificado ante la Secretaría.- Esto se hace para verificar la validez, suspensión o revocación del certificado así como para tener un acervo de los certificados que se emiten.

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

En relación al inciso A, apartado II del anterior artículo, la Secretaría de Economía expidió "las reglas generales a las que deberán sujetarse los prestadores de servicios de certificación.[101]" cuando se habla de elementos humanos se hace referencia al grado académico de la persona y a su carrera profesional. Por ejemplo, si es del área jurídica, por lo tanto debe ser licenciado en derecho o abogado con título, con experiencia de dos años en materia de personalidad e identidad de personas, mercantil notarial o de correduría pública. Considero que aquí existe una discrepancia con la ley, primero por que el artículo 100 del Código de Comercio señala quiénes pueden ser prestadores de servicios y no menciona en absoluto a un licenciado en derecho; claro que hay que interpretar la ley y podemos concluir que para ser notario hay que ser licenciado en derecho, pero es mejor que esté bien definido quién puede ser un prestador de servicios, ya que también se hace referencia a las personas morales y no se especifica en el mismo artículo que sean

[101] "Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación", Secretaría de Economía. publicado en el Diario Oficial de la Federación el 4 de Agosto de 2004.

licenciados en derecho; segundo, el artículo 100 no menciona la profesión de la persona que quiere ser prestador de servicios sino que pide un abogado o licenciado en derecho y que tenga conocimientos de correduría o notaria, aunque los certificados podrán o no llevar fe pública.

En lo personal considero que aquí el legislador debió ser más claro y darle prioridad a cualquier persona de ser prestador de servicios, sin limitarla por la carrera que hubiese estudiado; si se quiere que los certificados tengan fe pública entonces que se acuda con notario o un corredor público, pero que siempre que ellos expidan un certificado que tengan estos la fe pública, que no exista la opción de llevarla o no.

Seguimos con el párrafo III del inciso A; la ley menciona que se debe tener procedimientos definidos y específicos para la tramitación del certificado y nos parece sencillo de entender, pero cuando la ley nos habla de "procedimientos", qué debemos de entender por esta palabra. El diccionario de la Real Academia Española lo define como "acción de proceder, método de ejecutar algunas cosas; en derecho, actuación de trámites judiciales o administrativos". Considero que el legislador lo que pretendía era inclinarse por el método de ejecutar y en este caso hablamos del programa que se emplea para poder expedir un certificado, como son el software y el hardware y quizá aquí creo que los abogados y licenciados en derecho no sabemos mucho al respecto de estos temas, de aquí la importancia de trabajar en conjunto los abogados y los ingenieros. Sería más adecuado que el prestador de servicios de certificación sea una persona moral porque debe de contar con una infraestructura tanto de programas de datos y de ejecución para elaborar los certificados y asimismo personal administrativo que se encuentren con las más amplias facultades para poder proveer estos servicios; al referirme a personal administrativo me estoy refiriendo a técnicos e ingenieros que tengan conocimiento en la materia, ya que la Secretaría de Economía se encargará de vigilar estas actuaciones.

En el párrafo VII del inciso A cuando se habla de inscribir el certificado existe otra discrepancia de la ley, pues no existe un reglamento o un artículo que defina qué va a suceder con los notarios, ya que ellos tienen que cumplir con las disposiciones de la Ley

del Notariado cuyo sistema del protocolo es muy rígido, pero nunca se hace mención a un protocolo electrónico, y mucho menos se menciona que con el puro hecho de inscribir el certificado en la Secretaría de Economía será suficiente porque aquí el notario contraviene la ley, si no asienta los actos que lleva a cabo en su protocolo.

Un notario responde por daños y perjuicios que haya ocasionado por no llevar protocolo y esto no es justo, sin embargo la Secretaría de Economía propone que cuando los notarios tengan que otorgar un responsabilidad civil contra daños y pérdidas de terceros la secretaría podrá acordar que se responsabilicen solidariamente el Colegio de Notarios o sus respectivas agrupaciones, pero esto también es injusto porque a las instituciones públicas y las personas morales de carácter privado no se les aplica las mismas penalidades, entonces éstos tendrían que responder con sus propios bienes; en este caso hay que encontrar un equilibrio para que no queden unos con más privilegios que otros.

4.7. Eficacia transfronteriza de los certificados

Se presenta un problema muy común en cuanto a los certificados en las comunidades europeas, este es el caso de que una vez que se plantea todo el sistema para llevar a cabo la creación de los certificados y tenemos una regulación completa en cuanto a firma electrónica se plantea la pregunta: ¿Tienen eficacia los certificados extranjeros?

En Europa existe un principio de no discriminación que conduce a admitir que prestadores de servicios de certificación extranjeros puedan establecerse o prestar servicios locales siempre y cuando respeten las mismas normas aplicables a los prestadores de servicios nacionales.

Esto es un problema que se presenta en las comunidades europeas y que posiblemente aquí en México al momento de legislar podría pasar por desapercibido lo que sería lamentable ya que no tendríamos el conocimiento suficiente para saber si son eficaces o no, mientras que en Europa contemplan la alternativa de establecer un régimen internacional de las firmas electrónicas.

Se plantea con ese régimen internacional superar las soluciones legislativas que únicamente consideran válidas las firmas electrónicas basadas en un certificado emitido por un prestador de servicios de certificación autorizado para operar en el foro. Este planteamiento supone una restricción innecesaria y a largo plazo menoscaba la posición competitiva y el atractivo del foro para el comercio electrónico, y lo que se busca es que cuando se emita un certificado de un prestador de servicios extranjero se despliegue en un determinado país los mismos efectos que los expedidos por prestadores de servicios nacionales.

El proyecto pretende integrar a todos los estados miembros para que el estado en el que está establecida la entidad que expide el certificado y aquél en el que pretende hacerse valer el certificado, formen parte de un marco de integración que garantice la eficacia de todos los estados miembros de los certificados expedidos por prestadores de servicios de cualquier parte, siempre y cuando se cumpla con la normatividad establecida para los certificados. Otra de las medidas que se puede adoptar es el reconocimiento de estos certificados extranjeros siempre y cuando exista un régimen convencional o bilateral en el país de donde proceda y además de esto se procederá a la creación de dos tipos de controles, uno es operar en el prestador de servicios extranjero y otro es operar en el propio certificado expedido; si es en el prestador se procederá a emitir la eficacia de sus certificados y si se escoge la segunda opción se avaluará por un prestador de servicios local acreditado en los llamados acuerdos de certificación recíproca.

En España, el artículo 7 del RDLFE dice: "La consolidación del comercio electrónico internacional reclama no sólo que certificados expedidos por prestadores establecidos en España pueden ser eficaces en el extranjero sino que también que en España puedan serlo otros expedidos por prestadores establecidos en el extranjero".

En Alemania, el artículo 15 de la Gesetz Digitalen Signatur de 1997 limita las firmas digitales y las equipara con las basadas en un certificado procedente de cualquier otro estado miembro de la Unión Europea o del espacio económico europeo que satisfacen

las mismas condiciones de fiabilidad al tiempo que prevé la posibilidad de que la misma solución se extienda a otros estados en virtud de convenios multilaterales o bilaterales.

Los certificados que proceden de la Unión Europea operan con el principio de prohibición de restricciones y de no discriminación; según el artículo 4 del RDLFE esto hace más fácil la participación en los sistemas de acreditación de prestadores de servicios de certificación y de productos de la firma electrónica.

El artículo 29 del Reglamento del 21 de febrero del año 2000 reconoce la eficacia de los certificados seguros de creación o de verificación de firma electrónica siempre y cuando "hayan sido expedidos por los organismos designados para ello por Estados miembros de la Unión Europea o por otros Estados cuando un acuerdo internacional de reconocimiento mutuo vinculante para España así lo disponga."

CAPÍTULO V
PROCESOS DE LAS FIRMAS DIGITALES

SUMARIO.- 5.1.- Proceso general de la firma digital 5.2.- Normatividad de firma electrónica del Parlamento Europeo y del Consejo 5.3.- Normatividad de la firma electrónica en México 5.4.- El papel del notario mexicano en la firma electrónica.

5.1. Proceso general de la firma digital

Una vez que hemos visto de manera específica el funcionamiento del sistema de firma electrónica ahora tenemos que saber cómo funciona técnicamente en una computadora y de manera clara el funcionamiento de la firma digital así como de las partes que intervienen.

Repasando un poco todo lo que he mencionado en este documento sólo queda dar un breve repaso de manera general de la firma electrónica en diferentes ámbitos internacionales, tanto europeo como en la legislación mexicana.

El maestro José Niño de la Selva,[102] nos dice al respecto cuáles son los personajes que intervienen en una firma digital:

c) El usuario, que genera en sus computadoras dos claves una pública y otra privada.

d) Un agente certificador, este agente es un notario que se encarga de verificar la personalidad del usuario y genera un pre-certificado.

e) La autoridad certificadora, que aquí, en México, sería la Secretaría de Economía que se encarga de verificar el pre-certificado, generar el certificado y mandarlo a registrar.

[102] NIÑO DE LA SELVA, José. "El Notario Cibernético" Asociación Nacional de Notarios mexicanos A. C.

f) La autoridad registradora; esta autoridad automáticamente pide información a la ARC y registra el certificado en su base de datos y a su vez envía el registro a la autoridad certificadora.

e) La autoridad certificadora, una vez que tiene el certificado ya registrado, se lo envía al notario que lo solicitó.

f) El agente certificador, que es el notario, entrega al usuario el certificado ya registrado.

g) El usuario toma su certificado registrado por el notario y firma el acta notarial correspondiente.

Una vez que tenemos todo este procedimiento, como ya lo hemos visto, quedan aún procesos por realizar y necesitamos autentificar la firma con el certificado digital para esto únicamente necesitamos llevar a cabo tres pasos más:

b) El usuario envía su documento con la firma electrónica y su certificado digital.

c) El usuario receptor verifica la autenticidad del certificado y que se encuentre en la lista de los registrados, obtiene la clave pública del certificado y verifica la firma.

d) La autoridad registradora tiene la lista de certificados emitidos y la ofrece a los usuarios de manera electrónica.

De manera general, todo lo que hemos visto del proceso de una firma digital hace suponer que si seguimos el sistema tal y como se plantea tendremos un sistema perfecto e incorruptible de firma electrónica.

5.2. Normatividad de la firma electrónica en el Parlamento europeo y del Consejo

El 13 de diciembre de 1999 el Parlamento europeo y el Consejo de la Unión Europea deliberaron un marco comunitario para la firma electrónica.

En Europa se crea esta normatividad de la firma electrónica debido a las necesidades de la vida diaria que han evolucionado con la tecnología por lo que era importante el desarrollo y creación de la firma electrónica debido a las distancias tan cortas entre un estado y otro la manera de interactuar más rápido era a través de internet.

El fin último que persigue esta ley es la de autenticar las firmas de los actos que se lleven acabo a través de internet.

Lo que pretende la directiva es que se utilice este sistema y que no se cierre la sociedad a no aceptarlo, sino que se le de autorización y se lleve a cabo tal y cual se diseñó el sistema y de esta manera no fallará. La directiva respeta la libertad de las partes de actuar como mejor les convenga y poner condiciones generales para llevar a cabo la firma electrónica y aún así no se deberá de privar a las firmas electrónicas de su eficacia jurídica ni de su carácter de prueba en procedimientos judiciales.

La directiva de la Comunidad Europea trata con esta legislación que no se malinterprete la normatividad electrónica afectando de esta manera los intereses de los particulares en los actos que lleven a cabo; sin perjuicio de lo establecido sobre firma electrónica no deberá de dañar en ningún tipo de sentido la eficacia de los contratos que se lleven cabo a través de firmas electrónicas, puesto que no se pretende legislar en materia de contratos ni normas que determinen el lugar en el que se considera celebrado.

Por todo esto es por lo que la directiva determinó que para que la firma electrónica funcionara como sistema, debería de aceptarse como un medio de prueba y autenticarla al igual que una firma autógrafa. Y debido a que para reconocerla se debe de basar en criterios

objetivos, esta legislación rige la determinación de los actos jurídicos en los cuales puede utilizarse.

El primer paso de las comunidades europeas era la creación de esta legislación en materia de firma electrónica. Se prevé a futuro que otros países que no sean europeos puedan crear legislación en materia transfronteriza para que pueda operar el comercio electrónico a nivel mundial sin que existan obstáculos que los limiten.

En España el 26 de julio del año 2002 se hizo público el segundo borrador del anteproyecto que define los efectos de la firma electrónica y no difiere del texto actual del RD –Ley. Algunos de los puntos que se tocan, son:

1.- La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y los documentos que la incorporen serán admisibles como prueba documental en juicio.

2.- Al documento que incorpore una firma electrónica que no reúna los requisitos de la firma electrónica reconocida o no se base en un certificado expedido por un prestador de servicios que haya sido acreditado, no se le negarán, por el mero hecho de presentarse en forma electrónica efectos jurídicos ni será excluido como prueba de juicio.

3.- Cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se estará a lo estipulado entre ellas.

Estos son algunos de los conceptos que se tratan en el nuevo proyecto de la Ley de Firma Electrónica, sin embargo en septiembre del año 2003 el Congreso de Diputados tramitó enmiendas planteadas al proyecto de Ley de Firma Electrónica que había sido elaborado por el Ministerio de Ciencia y Tecnología que persigue promover un uso más generalizado de la firma electrónica.

En España, la firma electrónica como ya lo habíamos visto con anterioridad, es una realidad desde 1999, fecha en que entró en vigor el Real Decreto Ley que la regulaba, pero el problema que se presenta es que a los ciudadanos españoles le sigue generando desconfianza, por lo que el Ejecutivo intenta potenciar la seguridad jurídica mediante una nueva ley que reemplazará al decreto de 1999. Con este nuevo proyecto legal se transpone en el derecho español la directiva comunitaria que refleja las lagunas del decreto.

Una de las aportaciones principales de este nuevo proyecto es el establecimiento de un marco básico para el establecimiento del documento nacional de identidad electrónica (DNI), que permitirá a los ciudadanos identificarse y firmar documentos en el ámbito telemático. Sin embargo, existen grupos de oposición que critican esto argumentando que el proyecto no detalla ni concreta las pautas y los límites en la regulación del DNI.

Otra novedad que incluye el proyecto es que contempla la emisión de certificados de personas jurídicas. La firma electrónica a diferencia de la manuscrita es susceptible de integrarse en procedimientos automatizados, sin intervención directa de una persona física. Según el Ministerio de Ciencia y Tecnología este concepto permitirá dotar a las personas jurídicas de más flexibilidad para utilizar las herramientas de firma electrónica, que será de gran utilidad sobre todo para las pequeñas y medianas empresas.

El Grupo Socialista en España admite que en el futuro la firma electrónica puede agilizar muchos trámites de las empresas, pero el PSOE (uno de los grupos opositores) advierte el riesgo de que la administración monopolice la prestación de servicios de certificación a través de dos grandes servidores. La Fábrica de la Moneda y el Ministerio de Interior.

El proyecto de Ley presenta otra novedad, que consiste en la eliminación del Registro de Prestadores de Servicios de Certificación, que estaba previsto en el decreto de 1999. Puesto que ahora la prestación no está sujeta a autorización previa, se han reforzado las capacidades de control e inspección del Ministerio de Ciencia y Tecnología.

5.3. Normatividad de la firma electrónica en México

En México, el Congreso decretó el Proyecto de Decreto por el que se Reforman y Adicionan Diversas Disposiciones del Código de Comercio en Materia de Firma Electrónica y lo publicó en el Diario Oficial de la Federación el día 29 de agosto del año 2003.

En este decreto básicamente se adopta la esencia de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL). El congreso considera que esta ley reúne todas las expectativas y estudios de muchos países del mundo ya que los ampara la comisión de la Organización de las Naciones Unidas, como anteriormente ya lo habíamos mencionado.

De la misma manera que la directiva del Consejo de la Comunidad Europea, el Congreso plantea que la base de este sistema es el comercio electrónico que se está desarrollando en estos momentos a nivel mundial y que ésta es la razón por la que nos hemos visto obligados adoptar la legislación.

Sin embargo existen artículos dentro de la legislación mexicana que sirvieron de base para empezar a legislar sobre firma electrónica; algunos de ellos son:

a. **La Ley del Mercado de Valores.** En su artículo 91 dice: "... las partes podrán convenir libremente el uso de carta, telégrafo, télex, telefax o cualquier otro medio electrónico, de cómputo o de telecomunicaciones para el envío, intercambio o en su caso confirmación de las órdenes de la clientela inversionista y demás avisos que deban darse conforme a lo estipulado en el contrato, así como en los casos en que cualquiera de ellas requiera cualquier otra confirmación por esas vías..." Este artículo fue uno de los primeros en tener una reforma en cuanto al uso de medios electrónicos y da la pauta de que las partes puedan convenir el uso de los medios electrónicos o no, sin embargo ya anteriormente había señalado en el Capitulo I de

este documento, que él Código Civil Federal consagra en su artículo 1811, que cuando se trate de una propuesta hecha a través de medios electrónicos no se requerirá estipulación previa de los contratantes respecto de esto, por lo que se observa que es un poco contradictorio el artículo 91 de la Ley del Mercado de Valores debido a que aquí sí existe una estipulación previa, pero cuando se trata de una oferta a través de medios electrónicos, no.

b. **Ley de Instituciones de Crédito**. El artículo 52 expresa: "...las Instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público, mediante el uso de equipos y sistemas automatizados, estableciendo en los contratos respectivos las bases..... el uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y en consecuencia, tendrán el mismo valor probatorio.....". Si nos damos cuenta, este artículo le da la misma eficacia a una firma autógrafa que a una firma electrónica o digital.

c. **Ley Aduanera.** El artículo 36 dice "..... en los casos de las mercancías sujetas a regulaciones y restricciones no arancelarias cuyo cumplimiento se demuestre a través de medios electrónicos, el pedimento deberá incluir la firma electrónica que demuestre el descargo total o parcial de esas regulaciones o restricciones"..... Aquí en este artículo volvemos a retomar el tema de la firma electrónica que ya expliqué con anterioridad en capítulos anteriores; sin embargo no hay que dejar pasar que también entran los certificados ya que con éste, se demuestra el vínculo que existe entre el firmante y los datos de creación de firma, con la finalidad de averiguar de quién procede.

d. **Ley General de Sociedades Mercantiles.** El artículo 178 en su parte final dice: "Que en lo no previsto en los estatutos serán aplicables en lo conducente las disposiciones de esta ley" lo que significa que si llegara a hacerse uso de la aplicación de esta ley y no se encontrara tampoco la regulación que se busca, será el Código de Comercio el que lo suplirá y por lo tanto se pueden aplicar en su caso los artículos reformados en cuanto a comercio electrónico.

5) **El Código de Comercio.** 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, y los adicionales 89 bis, 90 bis y 91bis hablan sobre el comercio electrónico de acuerdo a las reformas que fueron publicadas por el DOF el 29 de agosto del año 2003 y comenzó su vigencia a partir del 29 de noviembre del mismo año.

En estas reformas al Código de Comercio, como ya lo expliqué con anterioridad, se tocan los temas del comercio electrónico: mensajes de datos, la firma electrónica, así como las partes que participan en la misma y los prestadores de servicios de certificación. Quizá por el momento sean las únicas reformas al Código de Comercio, aunque existe también el Reglamento al Código de Comercio en materia de Prestadores de Servicios de Certificación, donde se tipifican los lineamientos para ser prestador de servicios y sus actuaciones como tales.

También existen otras reformas en materia de comercio electrónico que vale la pena señalar:

1) 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 Federal de Procedimientos Civiles del Código de Comercio y de la ley Federal de Protección al Consumidor, todo esto publicado en el Diario Oficial de la Federación el 29 de mayo del año 2000.

Se puede decir que estas reformas junto con las del Código de Comercio del año 2003 fueron las que más empuje le dieron al comercio electrónico en materia legislativa.

2) Ahora se encuentra en el congreso la Iniciativa de Reformas y Adiciones sobre Diversas Disposiciones del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal. Esta iniciativa que todavía no está promulgada, trae las disposiciones en materia de delitos que tienen que ver con medios electrónicos como son: violación de correspondencia, fraude, informáticos y materia de derechos de autor.

3) Las últimas reformas y quizá, en cuanto a procedimiento, unas de las más importantes, son las que se hicieron al Reglamento del Registro Público del Comercio donde se asentaran todos los actos mercantiles a través de medios electrónicos. Este reglamento se encarga de describir el procedimiento que se llevará a cabo para la captura de éstos de manera electrónica.

5.4. El papel del notario mexicano en la firma electrónica

En México, a Asociación Nacional del Notariado Mexicano A. C. junto con la Secretaría de Economía, celebró un convenio sobre programas de modernización registral y de economía digital.

¿Quién estará a cargo de que cumpla con sus obligaciones? La Secretaría de Economía será el Registro Público de Comercio en coordinación con las autoridades responsables del Registro Público de la Propiedad en las entidades federativas, y éstos operarán a través de un programa informático donde almacenarán información registral. El objeto principal que se persigue en este convenio es que entre la ANNM y la Secretaría de Economía se lleven a cabo los principales objetivos:

I.- Un programa de modernización registral en cuanto a la captura del acervo histórico del Registro Público del Comercio, el uso de internet y de la firma electrónica para el envío y consulta de la información al registro público y de comercio; a este programa le nombraron SIGER.

II.- El programa de economía digital, en su emisión de certificados digitales y en la difusión de su uso.

III.- Es una obligación de la secretaría colaborar con la ANNM e insertar en su página de internet los servicios que ofrecen éstos en cuanto al programa de economía digital.

Existen otros puntos, sin embargo éstos son los que más nos interesan, puesto que aquí es donde se define el papel de la autoridad certificadora con el agente certificador, que en este caso el primero será la Secretaría de Economía y el segundo será el notario. El convenio no es muy extenso y se limita a cosas muy generales, no describe de manera explícita las funciones tanto del notario como de la Secretaria de Economía, pero estas lagunas quedarán complementadas con el Reglamento al Registro Público de Comercio donde se señala la manera en que se deberá de llevar a cabo el procedimiento de captura de los actos mercantiles.

De hecho en la Minuta Proyecto, en la que se reforman diversas disposiciones al Código de Comercio en su artículo 89 se define:

> 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.

En este artículo se ve claramente que la autoridad a la que le atribuyen la facultad de certificar los certificados digitales es la Secretaría de Economía y el artículo 100 de la misma minuta nos fundamenta la facultad del notario de prestar su servicio como agente certificador.

PROPUESTA:

La Secretaría de Economía publicó "Las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación"; Dichas reglas se limitan únicamente a describir los elementos humanos, materiales y económicos, así como los tecnológicos que tendrán que cumplir los prestadores de servicios de certificación. Sin embargo, la secretaría solicita elementos muy específicos, prácticamente una infraestructura de plantel donde colaboren profesionistas, tanto abogados como ingenieros, que tengan cierto nivel de conocimiento de elementos como el hardware y el software. A su vez, éstos deberán tener personal calificado para este tipo de prestación de servicios, así como mecanismos de seguridad para que no se filtre información y evitar robos, mal uso, etcétera.

Esta infraestructura no la tiene ni un corredor ni un notario. Si quisiera prestar un servicio de certificación, tendría que cumplir con todas estas normas, lo que considero absurdo, los notarios y los corredores se deben de regir por otro tipo de reglas especiales, que no sean estas reglas generales para todos los prestadores de servicios de certificación, sino un reglamento especial para las personas morales que quieran ser prestadores de servicios y que no tienen nada que ver con notarías y correduría.

Por su parte, la Ley del Notariado, no habla nada de certificaciones electrónicas, o firmas electrónicas. Para ellos no existe un ordenamiento que pueda reglamentar su actuación. Sin embargo, la Ley del Notariado del Distrito Federal, en su artículo 128, describe todos los actos que debe de contener una acta; son reglas especiales que se crean específicamente para que los notarios asienten los certificados electrónicos en un protocolo, así mismo que el notario lleve un protocolo especial (electrónico), de tal forma que se pueda dejar asentado que sí se llevó a cabo un acto. Sí existieran errores de nombres, de ortografía, que no causaran la nulidad de los certificados, debe verse la manera de enmendarlos, esto está reglamentado tanto en las normas que van a regir a los notarios como el reglamento especial para llevar a cabo el procedimiento de firma electrónica.

El Reglamento del Registro Público de Comercio es el único reglamento que menciona la intervención del notario en el programa de captura, debido al hecho de que en este programa se inscriben todos los actos de comercios que se lleven a cabo de manera electrónica. El Registro Público en el Código de Comercio en su artículo 21, sí regula la existencia de un folio electrónico por cada comerciante que realice actos de comercio. El registro público podrá autorizar a notarios o personas que soliciten el permiso para acceder a la base de datos de manera electrónica, por lo que este reglamento es una vez más una base para que exista un protocolo electrónico y normas especiales que rijan a los notarios en su actuar de manera electrónica. El artículo 5 del Reglamento del Código de Comercio dice que el notario que esté autorizado podrá enviar a través de medios electrónicos al programa SIGER del Registro Público de Comercio, el acta o póliza del acto a inscribir, pero una vez más volvemos a lo mismo ¿dónde está el reglamento del notario que lo califica para realizar actos a través de medios electrónicos? No existe una regulación específica para el notario que lo autorice. Esto es precisamente lo que propongo, reglas específicas que regulen este tipo de actuaciones.

CONCLUSIONES

PRIMERA.- La firma electrónica ha evolucionado en el ámbito del derecho y, a la par, de la tecnología. Esta última nos ha llevado a los límites de la creación de contratos a través de medios electrónicos: hemos pasado de la firma manuscrita a la firma electrónica.

SEGUNDA.- Se pone en duda si la firma electrónica tiene eficacia jurídica. La respuesta a esto es que sí la tiene ya que el uso de ésta permite llevar a cabo transacciones comerciales a través de internet, así como actos jurídicos siempre y cuando la firma cumpla con los requisitos legales de forma en los contratos.

TERCERA.- La firma electrónica tiene que cumplir con las normas establecidas para su eficacia jurídica, muy en especial en el ámbito de los contratos ya que una de las solemnidades de un contrato es que sea por escrito, por lo que aquí cobra fuerza la actividad notarial desempeñando funciones muy importantes en el comercio electrónico.

CUARTA.- La firma digital goza de la equiparación a la firma manuscrita ya que debe de contar con los principios de autenticidad, integridad y no debe de ser repudiable, por lo que interviene el notario para darle validez a la firma; la firma electrónica puede ser determinante de la presencia de una firma manuscrita en algún momento.

QUINTA.- No se deberá de confundir a un prestador de servicios con un notario ya que el prestador de servicios realiza algunas funciones iguales pero con un fin diferente al que busca usualmente el notario.

SEXTA.- El papel principal de un notario es la autenticación notarial de la firma digital que en su caso se encontrará ya certificada y que es relevante para asegurar la fiabilidad de ésta en un acto jurídico o de comercio, excluyendo cualquier tipo de fraude en la firma o el empleo de falsificación de clave privada.

SÉPTIMA.- Otro de los papeles a desempeñar por parte del notario es la manifestación de que la firma digital ha sido introducida por el titular en presencia del notario, comprobación de la identidad del titular, de la validez de la clave y de que el documento firmado corresponde a la voluntad de las partes y está conforme a derecho.

OCTAVA.- Los documentos públicos y privados son susceptibles de inscripción habiendo utilizado en el documento una firma electrónica avanzada y estando autorizado por un notario, es un documento auténtico que hace fe de su contenido.

NOVENA.- Hay que tener en cuenta que una buena regulación de las firmas electrónicas se puede hacer a través de la determinación de sus efectos jurídicos porque éstos repercuten tanto en los negocios jurídicos como en las declaraciones de voluntad que ésta a su vez se puede pronunciar en diferentes ramas del derecho, por ejemplo, administrativa, fiscal, civil, mercantil, etcétera.

DÉCIMA.- En países de la comunidad europea la firma electrónica es susceptible de prueba de los mensajes de datos, siempre y cuando cumpla con que está basada en un certificado reconocido y producida por un dispositivo seguro de creación de firma; si faltan estos requisitos no será excluida del juicio por el hecho de presentarse en forma electrónica.

DÉCIMA PRIMERA.- Los mensajes de datos en España también son emitidos como prueba, siempre y cuando no se tenga otra prueba mejor y se puedan dar todas las circunstancias necesarias para acreditar la autenticidad de los ficheros electrónicos del contenido de discos de los ordenadores o procesadores y que se garanticen con las pruebas periciales necesarias, así como la autoría de la firma electrónica utilizada y se le dará plena virtualidad jurídica.

DÉCIMA SEGUNDA.- El procedimiento de una firma digital, en resumen, consiste en que el usuario genera en su computadora sus claves pública y privada, lleva su clave pública a certificar con un agente certificador, quien es un notario y éste da fe de que la persona es quien dice ser y que acepta como suya una clave pública y elabora un precertificado. Enseguida va con una autoridad certificadora y ésta es la entidad encargada de verificar el precertificado, de emitir los certificados solicitados por sus agentes certificadores y de enviarlos a registrar. La autoridad registradora realiza y guarda el registro de los certificados emitidos por las autoridades certificadoras y publica de manera electrónica la lista de los certificados emitidos, de aquí se envía a la autoridad registradora central encargada de guardar los registros de los certificados emitidos por las autoridades certificadoras y las listas de los certificados registrados por las autoridades registradoras.

DÉCIMA TERCERA.- Proceso general de una firma electrónica: primero, el emisor opta por mandar un mensaje y obtiene la clave asimétrica, ésta se adquiere en su propia computadora; a su vez se aplica un hash al texto, esto es, antes de encriptar el mensaje, se encripta el mensaje con la clave simétrica, se encripta el hash con la clave privada, se une el mensaje y el hash con la clave pública del receptor se encripta la clave simétrica, se añade al mensaje y se envía. El receptor recibe el mensaje y desencripta la clave asimétrica con la clave privada del emisor, desencripta el mensaje con llave asimétrica, se aplica el hash sobre el mensaje desencriptado y si no hubo modificación en el mensaje y los dos hashes corresponden, por lo que es auténtico y veraz.

DÉCIMA CUARTA.- Los certificados digitales deben vincular la clave pública a una persona determinada (ésta es su función principal), por lo que debe de identificar eficazmente al solicitante; debe de haber un control sobre la clave privada para que no sea susceptible de falsificarse, tienen que existir sellos temporales digitales de confianza esto es esencial para que funcione bien el sistema de certificación a fin de determinar el momento de creación de mensajes electrónicos durante el periodo de validez del certificado. El certificado debe de estructurarse de manera tal que sean válidos entre diversos países ya sea

a través de un convenio donde exista algún tipo de reconocimiento internacional del certificado o una conexión con autoridades de certificación.

DÉCIMA QUINTA.- Como dato cultural y estadístico en cuanto a firma electrónica, el Colegio de Abogados de Madrid ya ha recibido 1,500 solicitudes para registrar la firma electrónica. Los usuarios podrán enviar y recibir correos electrónicos cifrados y firmados que permitirán al destinatario verificar la autenticidad del remitente y comprobar también que el contenido del correo no ha sido modificado. En menos de 30 minutos y por 40 euros un abogado español podrá conseguir en su colegio la tarjeta necesaria para registrar su firma.

GLOSARIO

A distancia

Es un servicio prestado sin que las partes estén presentes simultáneamente.

Autenticación

Proceso por el cual se garantiza que el usuario que accede a un sistema de ordenador es quien dice ser. Por lo general, los sistemas de autenticación están basados en el cifrado mediante una clave o contraseña privada y secreta que sólo conoce el auténtico emisor.

Cifrado

Transformación de un mensaje en otro, utilizando una clave para impedir que el mensaje transformado pueda ser interpretado por aquellos que no conocen la clave.

Comercio electrónico

Todas las transacciones comerciales realizadas a través de internet en las que intervengan personas físicas.

Correo electrónico (e-mail) o servicio de mensajería interpersonal

Es el servicio más utilizado de internet. Permite la creación y transmisión de mensajes entre usuarios de la red sin que se requiera que estén conectados simultáneamente.

En este servicio no está garantizado que los mensajes siempre lleguen a su destino, ni que se informe de este hecho al remitente o que este último sea quien dice ser.

Confidencialidad

Característica o atributo de la información por el que la misma sólo puede ser revelada a los usuarios autorizados en tiempo y forma determinados.

Conversación electrónica (chatting)

Se trata de un servicio que permite la conversación simultánea entre varios usuarios a través de la red. Funciona mediante la conexión a un servidor en el que se elegirá un grupo de conversación o canal. Cada participante se da a conocer a los demás a través de un seudónimo o "nickname". Si el programa de conversación está preparado para ello, se pueden utilizar, además del intercambio escrito, servicios de conversación oral y videoconferencia.

Cookies

Conjunto de datos que envía un servidor web a cualquier navegador que le visita, con información sobre la utilización que se ha hecho, por parte de dicho navegador, de las páginas del servidor, en cuanto a dirección IP del navegador, dirección de las páginas visitadas, dirección de la página desde la que se accede, fecha, hora, etcétera. Esta información se almacena en un fichero en el directorio del navegador para ser utilizada en una próxima visita a dicho servidor.

Criptografía

Es la ciencia que mediante el tratamiento de la información, protege a la misma de modificaciones y utilización no autorizada. Utiliza algoritmos matemáticos complejos para la transformación de la información en un extremo y la realización del proceso inverso en el otro extremo.

Directorios de correo

Conjunto de direcciones de correo electrónico, estructurado para la realización de búsquedas. Es un concepto similar al de "guía telefónica", aplicado a las direcciones de correo electrónico.

Destinatario del servicio

Cualquier persona física o jurídica que utilice un servicio de la sociedad de la información por motivos profesionales o de otro tipo y especialmente para buscar información o para hacerla accesible.

Firma digital

Información añadida o transformación cifrada de los datos que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación.

FTP (File Transfer Protocol)

Es el nombre conjunto para designar los protocolos y programas que hacen posible el desplazamiento de ficheros entre dos ordenadores conectados a internet, con independencia de cuál sea el formato de los ficheros.

Grupos de noticias (Newsgroups, Netnews, News o Usenet)

Es un sistema de distribución global que permite crear foros de discusión sobre temas de interés. Se organiza en jerarquías como: comp (informática), soc (temas de interés social), biz (temas de negocios), alt (grupos alternativos) y otros de ámbito geográfico o sectorial. Hay diferentes programas para acceder a estos grupos de discusión, aunque tienden a incluirse en los navegadores principales. En ocasiones se puede acceder a ellos vía correo electrónico, convirtiéndose prácticamente en Listas de Distribución.

HTTP (Hyper Text Transfer Protocol)

Este es el que rige el intercambio de mensajes entre el cliente o navegador que se esta utilizando y el servidor al que se conecta y en el que se encuentra la información que se solicita. Protocolo de comunicaciones utilizando por los programas clientes y servidores de WWW para comunicarse entre sí.

HTML (HyperText Markup Language)

Lenguaje en el que se escriben los documentos a los que se acceden mediante los navegadores WWW. Admite componentes hipertexto y multimedia.

Integridad

Garantía de la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

Proveedores de servicios de internet

La función principal de estos proveedores es hacer posible la conexión a internet, y a su vez hacen prestaciones adicionales a los usuarios como la posibilidad de almacenar en su ordenador central el correo electrónico del usuario, la puesta a disposición de espacio en el disco fijo de su ordenador para páginas web del cliente, incorporar la información que el cliente quiera difundir a través de las páginas web y proporcionar servicios ulteriores de apoyo, usualmente la separación entre proveedores de acceso a internet y suministradores de servicios, se pierde en la realidad, no se encuentra la distinción de lo que hace una y otro.

Prestador de Servicios

Cualquier persona fisica o jurídica que suministre un servicio de la sociedad de la información.

Prestadores del servicio de alojamiento o almacenamiento de datos

Ésta es la actividad que consiste en alojar o almacenar con carácter no meramente provisional, los datos facilitados por el destinatario del servicio; puede consistir también en el almacenamiento de los mensajes de correo electrónico que envía y recibe el destinatario del servicio o de los mensajes correspondientes a una lista de distribución o de uno o varios grupos de noticias.

PGP (Pretty Good Privacy)

Programa de libre distribución, escrito por Phil Zimermann, que impide, mediante técnicas de criptografia, que ficheros y mensajes de correo electrónico puedan ser interpretados por personas no autorizadas. Puede también utilizarse para firmar electrónicamente un documento o un mensaje, realizando así la autenticación del autor.

Proveedores de contenido

Personas u organizaciones que publican información de cualquier tipo en internet, ya sea utilizando recursos propios o los suministrados por un proveedor de acceso.

Por vía electrónica

Un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento y de almacenamiento de datos y que transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético.

Servicio

Todo servicio prestado normalmente a cambio de una remuneración a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

Suministradores de servicios en línea y suministradores de contenido

Son los que proporcionan información, a los adjuntos a sus sistemas, que funcionan como red propia, alojando páginas de terceros, y como vía de acceso a internet que contratan los proveedores, en la práctica son una vía muy frecuente por lo cuál los usuarios se conectan a internet.

Usuarios

En la actualidad, una de las principales razones por las que existe internet es gracias a la propagación y al uso que hacen día a día los usuarios, y cada vez son más los que participan en la red. En su origen se caracterizaba por constituir una comunidad homogénea integrada por investigadores. En la actualidad el punto resaltante es la heterogeneidad de los usuarios de internet. Su expansión en cuanto al ámbito comercial obliga a que participen y utilicen la red una variedad de usuarios desde investigadores hasta empresarios, amas de casa, etcétera.

Servidor Web

Es el programa que, utilizando el protocolo de comunicaciones HTTP, es capaz de recibir peticiones de información de un programa cliente (navegador), recuperar la información solicitada y enviarla al programa cliente para su visualización por el usuario.

Servidor Web seguro

Servidor Web que utiliza protocolos de seguridad (SSL, SHTTP o PCT) el ejecutar transacciones en él. Un protocolo de seguridad utiliza técnicas de cifrado y autenticación como medios para incrementar la confidencialidad y la fiabilidad de las transacciones.

World Wide Web (www)

Es una malla mundial que nos permite navegar a través de ella, de una manera rápida y sencilla. A esta parte de internet se accede mediante el protocolo HTTP (Hyper Text Transfer Protocol).

BIBLIOGRAFÍA

LIBROS:

Apol - Lónia Martínez Nadal, *La Ley de Firma Electrónica*, Civitas Ediciones, Madrid, 2000.

---------- *Comercio Electrónico, Firma Digital y Autoridades de Certificación*, 2ª ed., Civitas Ediciones, Madrid, 2000.

Andrew Nash, William Duane, Celia Joseph, Perek Brink, *PKI Infraestructura de Claves Públicas*, Mc Graw Hill, Colombia, 2002.

De Miguel Asensio Pedro Alberto, *Derecho Privado de Internet*, 2ª ed., Civitas Ediciones, Madrid, 2001.

Clemente Meoro Mario E. y Cavanillas Múgia Santiago, *Responsabilidad Civil y Contratos en Internet, su regulación en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Comares, Granada, 2003.

Téllez Valdés Julio, *Derecho Informático*, 3ª ed., Mc Graw Hill, México, 2003.

Enrigue Zuloaga Carlos, *Pacto Contractual y Contratos atípicos*, Porrúa, México, 2000.

De la Peza Muñoz Cano José Luis, *De las Obligaciones*, Mc Graw Hill, México, 1999.

Bejarano Sánchez Manuel, *Obligaciones Civiles*, 4ª ed., Oxford University Press, México, 1998.

Reyes Corripio Gil-Delgado Ma. *Los Contratos Infórmaticos*, Comillas, Madrid, 1999.

Rios Hellig Jorge, *La Práctica del Derecho Notarial*, 5ª ed., Mc Graw Hill, México, 2002.

Diccionario de la Real Academia Lengua Española, 22ª ed., Tomo I, Espasa Calpe, Madrid 2002.

Villoro Toranzo Miguel, Metodología del Trabajo Jurídico, Limusa, México, 1999.

Barceló Rosa Julia, *Comercio Electrónico entre Empresarios*, tirant lo blanch, Valencia, 2000.

Treviño García Ricardo, *Epítome de los Contratos*, Mc Graw Hill, México, 1994.

Davara Rodríguez Miguel Ángel, *Manual de Derecho Informático*, 5ª ed., Aranzadi, Navarra, 2003.

LEGISLACIÓN:

Código Fiscal de la Federación, última reforma publicada en el Diario Oficial de la Federación el 5 de enero de 2004.

Código de Comercio, Agenda Mercantil, 13ª ed., ISEF, México, 2004.

Código Civil Federal, Agenda Civil Federal, 4ª ed., ISEF, México, 2004.

Ley del Notariado para el Estado de Jalisco, http://www.congresojal.gob.mx/legislacion/Leyes/Civiles/ley_notar.html

Código Civil para el Estado de Jalisco.

Ley Orgánica 15/1999, de 13 de diciembre, de *Protección de datos de carácter personal*, disco óptico, Agencia de Protección de Datos, Madrid, 2003.

Constitución Política de los Estados Unidos Mexicanos, última reforma publicada en el Diario Oficial de la Federación el 29 de octubre de 2003.

Constitución del Estado Libre y Soberano de Jalisco, disco óptico, Librería Agustín Yánez, Congreso del Estado de Jalisco.

Ley del Mercado de Valores. Última reforma publicada en el Diario Oficial de la Federación el 28 de enero de 2004.

Ley de Servicios de la Sociedad de la Información, publicada con la última reforma a los anexos el 30 de abril de 2001 en el BOE.

MATERIAL ELECTRÓNICO:

Disco Óptico "Agencia de Protección de Datos", Madrid, 2003.

Recomendación del consejo de la OCDE "Lineamientos para la protección al consumidor en el contexto del comercio electrónico" http://www.oecd.org.

"Ley Modelo Sobre Comercio Electrónico aprobada en 1996 y modificada en 1996 por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL)" http://www.uncitral.org/spanish/texts/electcom/ml-ecomm-s.htm.

Boletín Oficial del Estado, BOE http://www.boe.es/g/es/

Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de Junio de 2000, directiva sobre el comercio electrónico., del Diario Oficial de las Comunidades Europeas.

Real Decreto Ley 14/99 de 17/9/99 sobre firma electrónica
http://www.mineco.es/admonelectronica/legislacion/RDL14_99%20.htm.

Directiva 1999/93/CE del Parlamento Europeo y del Consejo del 13 de Diciembre del 1999, por la que se establece un marco comunitario para la firma electrónica.

PUBLICACIONES PERIÓDICAS:

Puente Escobar Agustín, "La Protección de datos en el ámbito de las comunicaciones," *Revista de Actualidad Jurídica* de Aranzadi.

IRC (Internet Relay Chat)

Charla Interactiva Internet. Protocolo para conversaciones simultáneas que permite comunicarse entre sí a varias personas en tiempo real.

Listas de distribución (Mailing lists)

Es un servicio que se basa en el correo electrónico, formando grupos de personas con intereses comunes sobre temas específicos, que intercambian información respecto a los mismos a través de sus direcciones de correo. Cualquier mensaje enviado a la lista se distribuye automáticamente a todos los miembros del mismo e incluso, a veces, podría hacerse público a terceros.

Normas PEM (Privacy Enhanced Mail)

Correo con Privacidad Mejorada. Norma aplicable al protocolo de correo electrónico utilizado en Internet, que permite cifrar de manera automática los mensajes de correo electrónico antes de enviarlos. No es necesario invocar procedimientos separados para cifrar el mensaje de correo.

Notario electrónico (TTP, Trusted Third Parties)

Entidad pública o privada encargada de la emisión de certificados digitales que atestigüen la autenticidad de los propietarios de los mismos.

Operadores de telecomunicaciones

Son los que disponen de la infraestructura que permite la transmisión de datos, usualmente la manera en que todos los usuarios se conectan a internet es a través de la línea telefónica, por lo cual se enlaza el ordenador del usuario a un sistema conectado directa o indirectamente a internet por medio del proveedor de acceso.

Operadores de red

Entidad pública o privada que haga disponible la utilización de una red de telecomunicación.