UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

Trabajo de fin de carrera titulado:

LA FIRMA ELECTRÓNICA Y SU APLICACIÓN EN LA LEGISLACIÓN ECUATORIANA

Realizado por:

CHRISTIAN PUENTE GARCÍA

Como requisito para la obtención del título de

ABOGADO

QUITO, MARZO DE 2009

DECLARACIÓN JURAMENTADA

Yo, Christian Alfonso Puente García, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

…….…….

Christian Alfonso Puente García

DECLARATORIA

El presente trabajo de investigación de fin de carrera, titulado

LA FIRMA ELECTRÓNICA

Y SU APLICACIÓN EN LA LEGISLACIÓN ECUATORIANA

Realizado por el alumno

CHRISTIAN ALFONSO PUENTE GARCÍA

como requisito para la obtención del título de

ABOGADO

ha sido dirigido por la profesora

Dra. MARÍA CRISTINA VALLEJO

quien considera que constituye un trabajo original de su autor.

……..……..

Dra. MARÍA CRISTINA VALLEJO

Directora

Los profesores informantes

Dra. CAROLINA GARCÍA, y

Dr. GABRIEL RECALDE

después de revisar el trabajo escrito presentado,

lo han calificado como apto para su defensa oral ante el tribunal examinador.

……...…… ……

Dra. Carolina García Saltos Dr. Gabriel Recalde

Quito, 10 de marzo de 2008

INDICE

INTRODUCCIÓN……..... 1

Capitulo I

Consideraciones Generales…….. 3

1. Antecedentes…….. 3

1.1 La firma autógrafa…… 3

1.2 El Mercantilismo…….. 4

1.3 Revolución Digital…… 5

1.4 Trasfondo Internacional…… 7

1.4.1 Unión Europea……... 7

1.4.2 Naciones Unidas…… 9

1.4.3 Comunidad Andina…… 10

Capitulo II

Elementos y Seguridad de la Firma Electrónica…… 12

1. Firma Electrónica y Firma Digital…….. 12

1.1 Funciones de la Firma Digital……... 16

1.2 Efectos de la Firma Digital……... 18

1.3 Elementos…….. 19

2. Criptografía……. 20

2.1 Características……... 21

2.2 Criptografía Simétrica……... 22

2.3 Criptografía Asimétrica……. 23

2.4 Función Hash…… 25

3. Funcionamiento……... 27

Capítulo III

Certificados Electrónicos y Entidades Habilitadas…… 29

1. Certificados de Firma Electrónica……... 32

1.1 Contenido del Certificado……. 32

1.2 Certificados Emitidos en el Extranjero……. 35

2. Entidades de Certificación…….. 36
2.1 Tercero Vinculado……. 38
2.2 Emisión de Certificados…… 40
2.2.1 Clasificación de Procesos de Emisión……... 42
2.3 Proceso de Acreditación…… 42
2.3.1 Acreditación de un Tercero Vinculado…….. 46
2.3.2 Acreditación de Entidades Públicas……... 46
2.4 Contrato entre Entidad y Usuario…….. 47
3. Infraestructura de Clave Pública……. 48
3.1 Jerarquía Estructural……. 49

Capítulo IV

Implicaciones Jurídicas de los Mensajes de Datos……. 51

1. El documento…….. 51
2. Mensaje de Datos…… 53
3. Ámbito Jurídico……... 53
3.1 Reconocimiento Legal……..……..... 54
3.2 Incorporación por Remisión.……..……..... 55
3.3 Propiedad Intelectual……..……..... 55
3.4 Confidencialidad y Protección de Datos……..... 57
3.5 Desmaterialización de Datos……..……..... 58
3.6 Calidad Probatoria……..……..... 59
3.6.1 Presunción de Validez……..……..... 61
3.6.2 Valoración de la Prueba……..……..... 62
4. Servicios Relacionados……..……..... 62
4.1 Factura Electrónica……..……..... 62
4.2 Sellado de Tiempo……..……..... 63
4.3 Notificaciones Electrónicas……..……..... 64
4.4 Notario Electrónico…….... 65

Capítulo V

Consideraciones Finales…… 67

1. Ventajas de la Firma Electrónica……..…… 67

2. Desventajas de la Firma Electrónica……..... 69
3. Conclusiones……...……..... 71

BIBLIOGRAFÍA……..... 73

INTRODUCCIÓN

Aquella ley primitiva en la que el más fuerte prevalecía sobre el débil, donde la fortaleza radicaba en la imposición de la supremacía física, ya es obsoleto, inmoral y digno de sanción; en la actualidad este factor de poderío se ha transformado en el conocimiento y utilización de las nuevas tecnologías, ya que para sobresalir y ser competitivos es necesario estar a la vanguardia de la informática.

El Internet es considerado como el mayor deposito de información y vía efectiva de comunicación, donde su crecimiento es constante e inmenso. Gracias a él, las transacciones se han facilitado ya que sus usuarios son capaces de establecer vínculos de forma instantánea, reduciendo costos y acortando distancias, constituyéndose en la mejor herramienta para el desarrollo económico mundial.

Conforme vamos creciendo y nuestra interacción social va en aumento, hemos evidenciado como la informática simplifica tanto nuestras actividades productivas como sociales, llevándonos a la conclusión de que su estudio, entendimiento y desarrollo profundo son de vital importancia, por que estar al tanto de la mera búsqueda de información o de la comunicación electrónica básica, no son suficientes para alcanzar los verdaderos beneficios que el Internet nos brinda.

Como sabemos, el Derecho no es una ciencia estática, por el contrario, es de evolución asidua donde su dinamismo depende y avanza conforme el desarrollo social se acrecienta. El surgimiento de una nueva actividad, un artefacto o una naciente realidad humana conlleva la necesidad de tipificarlos legalmente, a fin de mantener el cometido de regulación y control humano que tiene el Derecho. Es por esta razón, que el ámbito tecnológico es de suma importancia jurídica, ya que este involucra y afecta a la gran mayoría de ramas, como a las actividades humanas.

Es innegable el avance informático desmesurado, donde la vigencia y efectividad de un logro técnico en poco tiempo es transmutado a un método obsoleto por el nacimiento de uno nuevo; en virtud de ello, es preciso para la sociedad contar con un marco jurídico de vigencia constante, para que el adelanto informático no afecte de manera inmediata al régimen jurídico. Es así que, la firma electrónica como medio de identificación de

autoría y portadora de reconocimiento y responsabilidad legal, en la actualidad instituye la vía más eficiente y moderna, pero con el pasar del tiempo aparecerá una nueva metodología que la vuelva inútil, dando como resultado su desuso, sin embargo, la esencia del proceso siempre será la misma, es decir, la determinación de identidad del emisor y receptor para darle un valor legal de sus transacciones a través de la Red sin importar cual sea la técnica que utilicen, logrando vigencia de la misma normativa legal.

Me he planteado como principal objetivo el inquirir en las legislaciones, técnicas y campos de aplicación, tanto internacionales como nacionales, que envuelve la aplicación de la firma electrónica, con el fin ulterior de determinar sus beneficios y falencias de toda índole.

El presente texto está conformado de cinco capítulos, en los cuales se ha procurado tratar la temática de mayor relevancia, cuyo contexto no versa de meras citas o transcripciones documentales, por el contrario, se lo ha destinado al razonamiento, síntesis y elaboración de nuevas teorías que beneficien a su aplicación; para esto, su desarrollo se encuentra enfocado de forma didáctica a fin de evadir la exclusión de lectores que carezcan de conocimientos básicos sobre el tema.

CAPÍTULO I

CONSIDERACIONES GENERALES

1. ANTECEDENTES

1.1 La Firma Autógrafa

La firma autógrafa históricamente ha tenido como concepto genérico y en sentido amplio, el de una palabra, pequeño mensaje o dibujo, que tiene como fin identificar, asegurar y autentificar la identidad de un autor o remitente, o como una prueba del consentimiento o verificación de la integridad y aprobación de la información contenida en un documento o similar. En la práctica, se la determina como el nexo vinculante entre el firmante y el documento, la cual se debe realizar con su propia mano, derivándose de aquí el nombre *firma manuscrita*. Con estas referencias la Real Academia de la Lengua dilucidó a la firma como "*nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido*"[1].

Conjuntamente con el establecimiento de la firma en la sociedad, se determinó en el mundo jurídico la responsabilidad que tiene ésta respecto a los actos con terceros, determinando así cuatro propósitos específicos los cuales debe cumplir:

En la Edad Media, Savigny estableció que "*la declaración escrita se hace poniendo el nombre propio debajo de un acto escrito, y la firma establece que el acto expresa el pensamiento y la voluntad del que lo firma*", esclareciendo de esta manera el primer elemento que consiste en el *Consentimiento* en cual radica la manifestación exterior de la voluntad autónoma de los individuos.

Como segundo elemento tenemos a la *Solemnidad*, que se la podría establecer como sustancial ya que es uno de los preceptos legales determinantes al tiempo de la formación de un acto jurídico; así mismo en la Edad Media la firma como sinónimo de solemnidad fueron utilizados sellos, marcas y signos, que se formaban con una cruz en la que se entrelazaban letras o rasgos, Carlomagno, que apenas sabía escribir, hacía firmar sus actos

[1] http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=firma

por un sellador oficial. Se cree que la exigencia de la firma, que contienen los Códigos, arranca en octubre de 1358 cuando Carlos V de Francia obligó a los notarios a firmar los actos en los que intervenían[2].

También se entiende a la firma como *Prueba*, ya que a través del rasgo distintivo que se coloca al final del documento lo vincula al signatario; como cuenta Brizzio, en Roma, el valor del instrumento privado derivaba del valor que se asignaba a la prueba de testigos, quienes firmaban el instrumento con las partes[3].

Finalmente la firma como propósito de *Forma*, ya que la firma es una condición esencial para la existencia de todo acto jurídico, siendo esta un requisito inexcusable de su validez.

1.2 El Mercantilismo

Instaurada la firma manuscrita en la sociedad y regulada por un marco legal, el cual desde sus inicios le otorgó derechos y obligaciones al signatario; de manera paralela el mercantilismo también tuvo su nacimiento y evolución en la humanidad, tanto los marcadores económicos, como el comercio, existen desde el inicio de la civilización, aproximadamente en el siglo XII surgió con fuerza, sustituyendo al sistema feudal y evolucionando del trueque. Este capitalismo, calificado de comercial, llega a consolidarse en el siglo XV gracias a las expediciones y travesías que se emprendían en busca de nuevos mundos. En tal virtud, con el descubrimiento de América, la economía logra una importancia excepcional por la entrada en Europa de ingentes cantidades de metales preciosos provenientes de aquellas tierras.

El orden económico resultante de estos acontecimientos fue un sistema en el que predominaba ante todo lo comercial, ya que el único objetivo era el de intercambiar bienes en lugar de producirlos.

Con el pasar del tiempo el comercio se acrecentó de manera significativa, los instrumentos técnicos se multiplicaban dando lugar así a varios instrumentos comerciales, entre ellos, las letras de cambio. De esta manera, el capitalismo comercial engendra al capitalismo financiero, mismo que contribuyó a una nueva acumulación de capital al provocar una circulación más activa de mercancías y dinero.

[2] Alterini, Atilio A., Contratos civiles, comerciales, de consumo. Teoría General, Ed. Abeledo Perrot, Buenos Aires, 1998, p. 299.
[3] Brizzio, Claudia R., La informática en el nuevo derecho, Ed. Abeledo Perrot, Buenos Aires, 2000, p. 9.

Ecuador formaba parte, desde 1614, del Virreinato del Perú, y a partir de 1739 pasó a pertenecer al Virreinato de Nueva Granada y tras muchos alzamientos e intentos, y después de lograda la paz de la Gran Colombia en 1829, Ecuador alcanzaría realmente su independencia en el año de 1830, fecha en la cual se elabora la primera Constitución Política de nuestro país.

Nuestra guerra de independencia tiene como fondo subyacente la apertura de mercados, libre navegación y el fomento del progreso, ya que lo que sucedía en el mundo, específicamente en Europa, era de mayor trascendencia en lo que respecta al ámbito mercantil, esto es entre la segunda mitad del siglo XVIII y principios del XIX, donde el Reino Unido en primer lugar, y el resto de la Europa continental después, sufren el mayor conjunto de transformaciones socioeconómicas, tecnológicas y culturales de la historia de la humanidad, desde el Neolítico[4], hasta la llamada Revolución Industrial.

La economía basada en el trabajo manual fue reemplazada por otra dominada por la industria y la manufactura. La Revolución comenzó con la mecanización de las industrias textiles y el desarrollo de los procesos del hierro. La expansión del comercio fue favorecida por la mejora de las rutas de transportes y posteriormente por el nacimiento del ferrocarril. La producción y desarrollo de nuevos modelos de maquinaria en las dos primeras décadas del siglo XIX facilitó la manufactura en otras industrias e incrementó también su producción.

El auge de este industrialismo naciente, a diferencia de la agricultura, no duraría miles de años, ya que aproximadamente a mediados o finales del siglo XX empezó la gestación de nuevas tecnologías, las cuales implicarían una profunda transformación en la humanidad.

1.3 Revolución Digital

A fines del siglo XX, la sociedad dio un giro total al comercio y las comunicaciones, de tal forma que nunca más iban a ser vistos de la misma manera, ya no eran las computadoras, ni las bases de datos, ni las comunicaciones telefónicas que permitían el contacto verbal instantáneo de polo a polo, era mucho mas que eso; el mundo se hizo mucho más pequeño y las fronteras cada vez más difusas. Satélites y kilómetros de fibra óptica mediante ceros y

[4] Nueva edad de Piedra, por contraposición al Paleolítico o Edad Antigua de la Piedra, es uno de los períodos en que se considera dividida la Edad de Piedra. El término fue acuñado por John Lubbock en su obra de 1865 que lleva por título *Prehistoric Times*. Inicialmente se le dio este nombre en razón de los hallazgos de herramientas de piedra pulimentada que parecían acompañar al desarrollo y expansión de la agricultura. Hoy día se define el Neolítico precisamente en razón del conocimiento y uso de la agricultura o de la ganadería.

unos ahora llegan a cualquier rincón del planeta, el envío y recepción de mensajes de datos, voz e imagen de manera instantánea se convirtió de sueño a realidad con el nacimiento del Internet y con él, la Revolución Digital.

Las comunicaciones se simplificaron, los enlaces comerciales se multiplicaron y las limitaciones se redujeron a una línea telefónica y un computador y así todos pasamos a formar parte del comercio electrónico, redefiniendo aceleradamente las formas de producir, vender y competir, en prácticamente todos los sectores productivos de bienes y servicios, acercando más a la gente a través de la innovación de las comunicaciones mundiales, lo cual posibilita cambios en todos los ámbitos de la actividad humana, por ejemplo la competitividad, el empleo y la calidad de vida de las naciones.

Con las nuevas tecnologías, conocidas como *Tecnologías de la Información y la Comunicación (TIC)*, el tiempo y la distancia dejan de ser obstáculos, las redes mundiales de información, como Internet no conocen fronteras. Sin embargo, la aparición del comercio electrónico obliga claramente a replantearse muchas de las cuestiones del comercio tradicional, surgiendo nuevos problemas, como el asegurar que las personas con las que está contratando son quienes dicen ser.

La incertidumbre de que la información que se envía o recibe no ha sido alterada durante la transmisión o el valor jurídico que tiene el soporte electrónico, dejando atrás el respaldo clásico de la escritura, también se constituían en problemas.

Es por estas necesidades que la sociedad ha emprendido una búsqueda por encontrar métodos que nos permitan interrelacionarnos a través del Internet con la seguridad de que los actos de comercio que se inicien sean seguros, garantizando la capacidad legal de los interlocutores, integridad del contenido de los mensajes, privacidad entre las partes, invulnerabilidad de la información y por último, y lo más importante, la existencia de un método que faculte sellar contratos, otorgando completa validez jurídica, obligando a las partes al cumplimiento de lo pactado, sin necesidad de la presencia física de ambos, utilizando únicamente su computadora, permitiendo celeridad y economía contractual, logrando así que el Internet a más de ser una herramienta publicitaria y un buscador de posibles contactos, se convierta en una sala de reuniones virtual por la cual se logren establecer convenios con plena validez legal con un solo clic.

Surge de esta manera la Firma Digital, que a grosso modo, sin aún adentrarnos a lo que es la firma digital, podemos decir que se planteó la utilización de criptografía asimétrica para evitar la alteración de la documentación otorgando a cada usuario dos llaves, una pública y

una privada; todo esto bajo el control de un tercero, legalmente autorizado, quien se encargaría de la administración y control de su funcionamiento, dándole así la validez jurídica que se necesitaba.

1.4 Trasfondo Internacional

Desde hace más de una década ha existido preocupación por parte de la mayoría de las naciones desarrolladas, por brindar un marco normativo adecuado para la utilización de medios electrónicos, entre las que se encuentra la firma electrónica, para así brindar seguridad jurídica.

1.4.1 Unión Europea

La Unión Europea planteó los lineamientos generales en torno de los cuales se enmarcan los proyectos normativos sobre firma digital, encriptación y promoción del comercio electrónico, los mismos que están contenidos en diversas resoluciones y comunicaciones del Parlamento y Consejo Europeos. Dentro de sus decisiones iniciales se encuentra la *Resolución del Parlamento Europeo de 1996*, en la cual mediante resolución A4-244/96 del 19 de septiembre de 1996, el Parlamento Europeo solicitó a la Comisión de Iniciativa Europea sobre Comercio Electrónico la elaboración de lineamientos referentes a la seguridad de la información, confidencialidad, la firma digital y la protección de la privacidad. Así mismo, en julio de 1997 la *Conferencia Ministerial Europea* ponderó sobre la necesidad de crear un marco legal y técnico para la firma digital en Europa; de esta manera se fue avanzando y en 1998, el 23 y 24 de abril se estableció la *Audiencia de la Unión Europea sobre firma digital y encriptación*, la cual tuvo como objetivo la exploración del uso y desarrollo de la firma digital y la encriptación.

Finalmente la *Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la firma electrónica*[5], redactó los criterios para el reconocimiento jurídico de firma electrónica, en los cuales se resalta los servicios de certificación, efectos jurídicos y la responsabilidad que acarrea su uso, otorgando de tal manera un marco legal amplio y suficiente para su correcta

[5] http://europa.eu/scadplus/leg/es/lvb/l24118.htm

aplicación, los cuales he considerado necesaria su lectura, ya que son los pilares de la firma electrónica en la legislación mundial, por lo tanto se incluye al Ecuador, estos criterios son:

La Directiva define dos nuevos conceptos:
«Firma electrónica avanzada», esto es, la firma electrónica que cumple los requisitos siguientes:
- estar vinculada al firmante de manera única;
- permitir la identificación del firmante;
- haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;
- estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable.

«Certificado reconocido», que debe constar de lo siguiente:
- la indicación de que el certificado se expide como certificado reconocido;
- la identificación del proveedor de servicios de certificación;
- el nombre y los apellidos del firmante;
- un atributo específico del firmante, en caso de que fuera significativo en función de la finalidad del certificado;
- los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del firmante;
- una indicación relativa al comienzo y fin del período de validez del certificado;
- el código identificativo del certificado;
- la firma electrónica avanzada del proveedor de servicios de certificación que expide el certificado.

Los proveedores de servicios de certificación que cumplan determinados requisitos contemplados en la Directiva pueden proporcionar también certificados.

Efectos jurídicos de la firma electrónica
La principal disposición de la Directiva establece que la firma electrónica avanzada basada en un certificado reconocido equivale a una firma manuscrita y es admisible como prueba en procedimientos judiciales.
Además, es imposible rechazar jurídicamente una firma electrónica por el mero hecho de que:
- ésta se presente en forma electrónica;
- no se base en un certificado reconocido;
- no se base en un certificado expedido por un proveedor de servicios de certificación acreditado;
- no esté creada por un dispositivo seguro de creación de firma.

Responsabilidad
Los Estados miembros velarán por que el proveedor de servicios de certificación que expida un certificado reconocido sea responsable, ante cualquier persona que de buena fe confíe en el certificado, a efectos de:
- la veracidad de toda la información contenida en el certificado reconocido;
- la conformidad con todas las prescripciones de la Directiva por lo que se refiere a la expedición del certificado reconocido;
- la garantía de que, en el momento de la expedición del certificado reconocido, obraba en poder del titular identificado en el mismo el dispositivo de creación de firma correspondiente al dispositivo de verificación dado o identificado en el certificado;

- la garantía de que, en caso de que el proveedor de servicios de certificación genere los dispositivos de creación y de verificación de firma, ambos funcionan conjunta y complementariamente.

El proveedor de servicios de certificación no debe responder por los daños y perjuicios causados por el uso de un certificado reconocido que exceda de los límites indicados en el mismo.

1.4.2 Naciones Unidas

Luego de cinco años de deliberaciones por parte de la Comisión para el Derecho Mercantil de las Naciones Unidas (CNUDMI), la cual siguió los mismos pasos y procuró repercutir el mismo éxito que se dio en 1996 con su Ley Modelo sobre Comercio Electrónico, pero ahora con el tema de la Firma Electrónica; consecuencia que no resultó tan novedosa como en 1996 que como vimos en el sub capítulo anterior, ya se ocuparon páginas en los diarios oficiales respecto al tema a nivel mundial; lógicamente, a pesar de ello, no se desaprueba la iniciativa y gran trabajo que tuvo la Asamblea General de las Naciones Unidas en su 56º Periodo de Sesiones de 12 de diciembre de 2001, celebrado en la ciudad de Nueva York, en el que se aprobó la Resolución 56/80 sobre la *Ley Modelo sobre las Firmas Electrónicas, de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*[6].

En el cuerpo legal precitado no se permite ni se limita exclusivamente al funcionamiento del comercio electrónico en un mercado limitado, como es el caso europeo, el cual es soslayado únicamente por las legislaciones de los Estados miembros, los cuales se reglan por sus propias normas de contratación; por lo tanto, el instrumento de las Naciones Unidas se encuentra redactado en un sentido mucho más amplio con objetivos mayormente extensos.

Dentro del texto en mención, se busca como objetivo principal, el desarrollar los principios fundamentales enunciados en el artículo 7 de la Ley Modelo sobre Comercio Electrónico[7] respecto al cumplimiento de la función de la firma en las operaciones de comercio electrónico, con miras a fomentar la confianza en la utilización de la misma, a fin de que

[6] http://daccessdds.un.org/doc/UNDOC/GEN/N01/490/29/PDF/N0149029.pdf?OpenElement

[7] 1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente. 2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

surtan efectos jurídicos cuando sean el equivalente funcional de las firmas manuscritas, ya que la Comisión dentro de sus deliberaciones tomó en cuenta de manera expresa el número creciente de transacciones comerciales internacionales que realizan por el medio del comercio electrónico.

1.4.3 Comunidad Andina de Naciones

Siendo la CAN conformada por cuatro países (Ecuador, Colombia, Perú y Bolivia) que tienen por objetivo común el alcanzar un desarrollo integral, más equilibrado y autónomo, mediante la integración andina, suramericana y latinoamericana, ha visto necesaria la discusión de temas fundamentales de comercio dentro de los cuales, obviamente, se incluyó el comercio electrónico. Es por esta razón, que a raíz de una solicitud dada por la Asociación de Empresas de Telecomunicaciones de la Comunidad Andina (ASETA)[8], en junio de 2002 se elaboró un trabajo de análisis comparativo y recomendaciones de armonización respecto a *Legislación sobre Comercio Electrónico en los Países Miembros de la Comunidad Andina*[9], estudio que fue realizado con el apoyo de la Unión Internacional de Telecomunicaciones (UIT), cuyo objetivo fue plasmar un instrumento de derecho comparado de la legislación vigente de los países miembros en relación al comercio electrónico, cubriendo las áreas de mensajes de datos, las firmas electrónicas, los certificados digitales y las Entidades / autoridades de Certificación y Registro, presentando en cada una de ellas un conjunto de recomendaciones, con el fin de lograr una armonía en las disposiciones legales.

Dentro del presente texto se reconoce la gran labor efectuada por la legislación peruana, ya que en su mayoría se recomienda el seguimiento de los parámetros dados en ésta, pero sin menospreciar el trabajo ecuatoriano ya que se registran puntos importantes que deben tomarse en cuenta, como es el valor probatorio que se le otorga a la firma digital y los lineamientos de extinción de la misma.

[8] Asociación de empresas operadoras de servicios de telecomunicaciones que en el marco de la Comunidad Andina coadyuva al desarrollo armónico de las telecomunicaciones, contribuyendo así con el proceso de integración.

[9] http://www.itu.int/ITU-D/cyb/publications/archive/Legislacion%20Comercio%20Electronico%20CAN1.pdf

Como podemos evidenciar respecto al tema, en el mundo grandes pasos ya se han dado en *corto tiempo*, pero aún nos queda mucho por recorrer. Es verdad que el Ecuador se encuentra *retrasado* pero ya hemos dado nuestros primeros pasos, y a este retraso lo debemos considerar más como una ventaja ya que tenemos la oportunidad de observar las huellas de quienes nos anteceden para repetir los aciertos y evitar los errores.

Actualmente nos encontramos frente a una verdadera revolución que está cambiando la forma de vida de la sociedad, la misma que además de infraestructura física, necesita nuevas iniciativas con verdadero potencial, ocho artículos constitucionales[10] no son suficientes para construir una sociedad que esté a la vanguardia de la informática. Requerimos de una política encaminada al desarrollo tecnológico del país, más que publicitar necesitamos empujar al comercio electrónico del Ecuador, al respecto ya mucho se ha opinado en nuestro medio con ciertos avances temerosos, lo que ahora necesitamos es pasar de la opinión a la acción.

[10] ***Constitución Política (2008)*** **Art. 16**.- Todas las personas, en forma individual o colectiva, tienen derecho a: **2.** El acceso universal a las tecnologías de información y comunicación.
Art. 17.- El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto: **2.** Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada.
Art. 262.- Los gobiernos regionales autónomos tendrán las siguientes competencias exclusivas, sin perjuicio de las otras que determine la ley que regule el sistema nacional de competencias: **6.** Determinar las políticas de investigación e innovación del conocimiento, desarrollo y transferencia de tecnologías, necesarias para el desarrollo regional, en el marco de la planificación nacional.
Art. 277.- Para la consecución del buen vivir, serán deberes generales del Estado: **6.** Promover e impulsar la ciencia. la tecnología, las artes, los saberes ancestrales y en general las actividades de la iniciativa creativa comunitaria, asociativa, cooperativa y privada.
Art. 298.- Se establecen preasignaciones presupuestarias destinadas a los gobiernos autónomos descentralizados, al sector salud, al sector educación, a la educación superior; y a la investigación, ciencia, tecnología e innovación en los términos previstos en la ley. Las transferencias correspondientes a preasignaciones serán predecibles y automáticas. Se prohíbe crear otras preasignaciones presupuestarias.
Art. 322.- Se reconoce la propiedad intelectual de acuerdo con las condiciones que señale la ley. Se prohíbe toda forma de apropiación de conocimientos colectivos, en el ámbito de las ciencias, tecnologías y saberes ancestrales.
Art. 334.- El Estado promoverá el acceso equitativo a los factores de producción, para lo cual le corresponderá: **2.** Impulsar y apoyar el desarrollo y la difusión de conocimientos y tecnologías orientados a los procesos de producción.
Art. 347.- Será responsabilidad del Estado: **8.** Incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales.
Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad: **1.** Generar. adaptar y difundir conocimientos científicos y tecnológicos. **2.** Recuperar, fortalecer y potenciar los saberes ancestrales. **3.** Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

CAPÍTULO II
ELEMENTOS Y SEGURIDAD DE LA FIRMA ELECTRÓNICA

Hemos visto en el Capítulo I, que la firma electrónica está siendo utilizada en varios países del mundo, ya que la práctica ha demostrado que es un medio por el cual se puede autenticar mensajes de manera segura y económica, con la cual se cerciora la confidencialidad entre emisor y receptor, certificando la integridad del mensaje, dando como resultado un flujo comercial con mayor celeridad y confiabilidad, en razón de que la firma ológrafa queda en un segundo plano dentro de esta nueva Revolución Digital.

Ahora que ya tenemos claro el ámbito general de la firma electrónica, daremos paso a los elementos particulares de ésta, estableciendo las diferencias que existen entre los términos "firma electrónica" y "firma digital" ya que como veremos, estos no son similares, pasaremos por la criptografía y su importancia, para finalmente analizar el funcionamiento de la firma como tal.

1. FIRMA ELECTRÓNICA Y FIRMA DIGITAL

La *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos* (Ley 67) la cual rige al Ecuador desde el año 2002, establece que la firma electrónica "son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos."[1112]. Como se desprende de la simple lectura del concepto precitado, el campo de aplicación es sobradamente amplio, ya que se ha definido a la firma electrónica como el conjunto de datos verificativos, directamente vinculados con un mensaje electrónico, los cuales permiten de forma veraz e innegable, la relación entre

[11] *Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de datos*; R.O. #557 del 17 de abril de 2002.

un mensaje y su emisor, convirtiendo a este último como único responsable de la información enviada.

De esta manera queda claro el reconocimiento y validez jurídica que tiene la utilización de la firma electrónica, sin importar el método o técnica que se utilice como medio de seguridad, por cuanto la variedad y complejidad de métodos criptográficos es bastante extensa. Esto vendría a constituirse en un acierto por parte de nuestros legisladores, ya que a mi consideración ellos deben haber tomado muy en cuenta el hecho de que nos encontramos en avances experimentales y no nos podemos regir a un método restringido de comprobación de autoría, sin saber cual será el medio apropiado que se acople a nuestra sociedad y mas aún sabiendo que la tecnología es una ciencia que avanza a pasos agigantados donde las técnicas quedan obsoletas en poco tiempo.

En la mayoría de los textos, por no decir todos, que tratan el tema de la firma digital, determinan a la firma electrónica como un género y la firma digital como la especie, esto en razón de que la firma electrónica está caracterizada por ser todo modo de identificación de autoría basada en medios electrónicos, en donde el autor tiene el propósito de ligarse con el documento. Sarra también lo establece así diciendo que es el "… identificador que va adosado (*atachado*) o lógicamente asociado a un mensaje electrónico, documento o datos, y los propósitos para los cuales fue incluido implican el concepto jurídico de firma"[12], el problema radica en que la autoría queda únicamente supeditada al simple hecho de que el emisor tiene el "propósito" de relacionarse con el mensaje que ha enviado, no existe ninguna certeza técnica que nos asegure que el instrumento no ha sido modificado al momento de su envío, y de la misma manera no existe un nexo legal que determine que el emisor es en verdad quien dice ser. Estas atribuciones fundamentales son de la firma digital, como ya lo explicaré en párrafos posteriores.

Para mayor claridad de lo que es la firma electrónica, Apolonia Martínez[13] explica que,

> "Una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita. este concepto amplio y tecnológicamente indefinido de firma (…) tendría cabida técnicas tan simples como un nombre u otro elemento identificativo incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de valor probatorio a efectos de autenticación, aparte de su nula aportación respecto a la integridad del mensaje…"

[12] SARRA, Andrea Viviana; *Comercio Electrónico y Derecho;* Ed. Astrea; Buenos Aires 2001; p. 389

[13] MARTÍNEZ Nadal, Apolonia; *Comercio electrónico, firma digital y autoridades de certificación*; 2ª Ed. Colección Estudios de Derecho Mercantil; Civitas; Madrid 2000; p. 40

se entiende tan simple y poco segura a la firma electrónica que perfectamente puede concebirse como una firma manuscrita digitalizada utilizada al final de un mensaje, con la cual se liga al emisor con el texto.

Por su parte la firma digital o firma electrónica avanzada, como se la conoce en algunas legislaciones internacionales, es un método mucho más técnico, cuyo sistema radica en la utilización de criptografía, esto en razón de que el fin último de la firma digital es la protección e inviolabilidad de la información que se envía debiendo necesariamente recurrir a la encriptación la cual se define, según la Real Academia de la Lengua, como el arte de proteger la información, deviniendo el término criptografía, del griego *kriptos* que significa oculto y *graphe* que representa a la escritura, resolviendo en que es el arte de escribir con clave secreta o de un modo enigmático.

En otras palabras, la criptografía es la transformación de mensajes en textos aparentemente ilegibles en donde únicamente el emisor y receptor consiguen resolverlos a su forma original, alcanzando así que cualquier persona que no posea la clave le sea imposible descifrarlo, por lo general su creación es a través de algoritmos[14]. Para tener más clara esta idea, la firma digital se la entiende como el registro electrónico a través de *criptografía asimétrica de clave pública* donde el receptor del mensaje tiene la posibilidad de verificar si la información que recibió ha sido alterada en algún punto contado desde el envío hasta su recepción.

La diferencia entre estos dos métodos de autentificación electrónica de autoría radica en que al momento de utilizar la firma digital se aplican presunciones *juris tantum* sobre la identidad del emisor o firmante y la integridad del documento que él suscribió, es decir, son presunciones legales que se las mantienen hasta que se presenten otras situaciones que demuestren lo contrario o se las vuelvan controvertidas. Para dejar claras estas presunciones, un ejemplo de esto es la presunción de legitimidad de los actos administrativos, que pueden ser desvirtuados por el interesado demostrando que los mismos violan el orden jurídico.

Para esclarecer totalmente la diferencia entre estos dos elementos de identificación me permito citar al doctor Alfredo Reyes Krafft, el cual a mi parecer mejor define estas herramientas decretando a la firma electrónica como los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que

[14] Un algoritmo según la Real Academia es el "conjunto ordenado y finito de operaciones que permite hallar la solución de un problema." Es decir, es el proceso, por lo general de ámbito matemático, que se utiliza para despejar una incógnita o resolver cualquier tipo de problema.

puedan ser utilizados para identificar y/o vincular al firmante en relación con el mensaje de datos, en forma equivalente a la firma manuscrita, y la firma electrónica avanzada como a la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control, conocida también como firma digital, que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste[15], nótese, como ya he repetido numerosas veces, en su primera definición se dice la posibilidad de vincular al signatario con el mensaje, esto podría ser cualquier símbolo, palabra o nombre que éste utilice con la única finalidad de identificador, dejando a un lado cualquier tipo de seguridad para el mensaje, resultando en un peligro de falsificación sencilla; y en su segunda definición se asevera el vínculo excluyente entre el firmante con el mensaje y brinda la tranquilidad del destinatario por cuanto cualquier modificación posterior al envío sería detectada.

Es normal la existencia de teorías contrapuestas en temas de relevancia, y ésta no es la excepción, existen juristas que sostienen que el calificativo de genero-especie entre éstas dos es totalmente erróneo, planteando el hecho de que lo "electrónico" es más restrictivo que lo "digital" ya que el primero se vincula a una tecnología específica y lo "digital" es el nombre con el cual se ha acordado para este tipo de información; además de esto, jurisconsultos argentinos como Mauricio Devoto, a quien tengo gran respeto y agradecimiento por su obra *Comercio electrónico y firma digital* cuya lectura ha sido de gran ayuda pero lo cual no significa que no tengamos pensamientos opuestos en ciertos temas, manifiesta su desacuerdo, mencionando que la firma escaneada que puede ser depositada al final de cualquier documento, carece de los requisitos mínimos de seguridad para otorgarle valor jurídico lo cual se contrasta en la firma digital.

Personalmente respaldo la conexión que existe entre firma electrónica y firma digital de género-especie ya que ambas son vías de identificación de autoría de mensajes de datos, las dos coexisten en un mundo tecnológico el cual se lo realiza a través de computadoras y tanto la una como la otra son utilizadas por millones de personas las cuales persiguen un mismo objetivo; obviamente la distinción radica en la seguridad que brindan, pero por esto no dejan de ser género-especie, el genero es la determinación de autoría del firmante y la especie es la determinación de autoría del firmante indudable, un ejemplo claro de esta relación es la de caballo como género y el caballo árabe de nombre Relámpago con doce

[15] REYES KRAFFT, Alfredo; *La firma electrónica y las entidades de certificación*; Ed. Porrúa; México 2003; p. 164

años de edad cuyo propietario es Pedro Pérez como especie, la esencia viene a ser la misma.

1.1 Funciones de la Firma Digital

La firma digital debe garantizar a sus usuarios cuatro puntos básicos:

- *Autenticidad* del emisor del mensaje: es la primera y fundamental función de la firma digital, ya que con ésta se le imputa la autoría innegable a quien suscribe el documento, además de conferirle todos los efectos jurídicos que ésta acarrea, esto por cuanto la relación inseparable que se genera entre firma y documento volviendo a estos en uno solo para garantizar tanto al firmante como a quien recibe, la no alteración que podría existir al momento de su envío.
- *Confidencialidad* del mensaje de datos entre emisor y receptor: función imperiosa dentro del mecanismo en razón de la inmensa cantidad de riesgos que existen en la Red; cuando nosotros enviamos un correo electrónico, a pesar de que la recepción del mismo se de en cuestión de centésimas de segundo, la seguridad de nuestro mensaje es totalmente vulnerable ya que el documento viaja en su formato original, es por esto que dentro de la firma digital cada usuario posee dos claves, una privada y una pública, la primera la utilizamos para encriptar el mensaje que hemos escrito, para así enviarlo al destinatario especificando la clave pública de este (identificable públicamente) determinando que éste será la única persona que pueda abrir el mensaje con la clave pública del emisor y la clave privada del receptor la cual a su vez desencriptará el mensaje emitiendo de manera inmediata una notificación en la cual conste que no ha sido alterado el mensaje original, dando como resultado la confidencialidad deseada entre ambos; más adelante hablaremos con mayor detenimiento sobre este proceso.
- *Integridad* del mensaje firmado: el documento firmado digitalmente debe ser íntegro, por lo tanto se garantiza que el contenido que el receptor recibe, es exactamente el mismo que aquel que el emisor envió firmado, de esta manera se asegura que cualquier modificación por terceros que pueda darse será evitada y el mensaje original sin alteraciones será recibido.
- *No repudio* por parte del firmante: la persona quien envía un mensaje de datos con firma digital no puede aducir que no lo ha enviado ya que técnicamente se puede demostrar la identidad única e inequívoca del emisor, esto por cuanto existe un vínculo

jurídico entre el usuario y un tercero de confianza o *Entidad de Certificación* la cual ha sido constituida legalmente y se encuentra bajo la regulación del Consejo Nacional de Telecomunicaciones (CONATEL), lo cual hace del signatario el único y total responsable del uso que éste de a la firma digital; menciono esto nada más como un adelanto de lo que trataremos en capítulos posteriores. Este punto es de vital importancia para el aumento de las relaciones jurídicas y comerciales entre personas por medio del Internet, ya que se permite una disminución inmensa en los costos transaccionales y la celeridad necesaria que se busca. Además de esto, con la incursión de responsabilidades legales para los usuarios se otorga valor probatorio de autoría a la firma digital. De igual manera, no existe la posibilidad de repudio por parte del receptor del mensaje.

Ahora bien, habiendo explicado las bondades de la firma digital, a continuación se ilustra un cuadro comparativo entre la firma manuscrita y la digital, para demostrar que a pesar de ser la firma autógrafa el medio de uso común y obligatorio por varios siglos, ésta tiene falencias claras que las cubre la firma digital, como es el caso de la confidencialidad y el no repudio, el primero lógicamente porque nuestra firma personal queda a vista y paciencia de todo documento que suscribimos, dejando de manifiesto nuestros actos y apartando del camino la confidencialidad que pudimos haber deseado. En segunda instancia el no repudio es un hecho claro que no sucede con la firma manuscrita, cualquier texto firmado puede su supuesto autor aducir que él no ha sido quien firmó el documento, deslindándose de cierta manera de cualquier responsabilidad, a pesar de que existan exámenes grafológicos los cuales también pueden ser inexactos, cosa que no sucede con la firma digital como ya lo expliqué anteriormente.

	Firma Manuscrita	**Firma Digital**
Elementos personales		
La firma como signo personal	SI	SI
Voluntad de asumir el contenido del doc.	SI	SI
Elementos Funcionales		
Integridad	SI	SI
Autenticidad	SI	SI
Confidencialidad	NO	SI
No repudio	NO	SI

1.2 Efectos de la Firma Digital

Dentro de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas aprobada en la 85ª Sesión Plenaria de 2001, reza en su artículo sexto que "Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica…"[16], dejando de esta manera claro el tratamiento igualitario que deberá darse a las firmas electrónicas en comparación con la firma manuscrita, dejando de lado cualquier restricción que pueda darse respecto de sus efectos jurídicos como firma.

Inspirado en este artículo, un año más tarde, dentro de nuestra ley de Comercio Electrónico se decide incorporar una norma similar en el artículo 14 la cual menciona que "La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba enjuicio.", reiterando de esta forma el valor legal que debe darse a las firmas electrónicas y resaltando además el factor de valor probatorio que tienen éstas dentro de un proceso judicial, pero más que nada, la similitud entre firma manuscrita y digital ante los ojos de la ley.

Explicado esto, cabe establecer los efectos que tiene la firma electrónica, las cuales tienen relación directa con sus funciones:

- *Presunción de autenticidad*: aquella firma electrónica que haya cumplido con el requisito de estar bajo el control de una Entidad de Certificación se decretará como verídica, determinando el vínculo jurídico que existe entre firma y autor resultando en la voluntad manifiesta de obligarse.
- *Presunción de integridad*: el proceso de firma digital se realiza con posterioridad al documento que vamos a enviar, esto en razón de que una vez firmado digitalmente el escrito será imposible su alteración ulterior ya que los dos, tanto firma como documento, se convierten en uno solo, valiéndose del *certificado* que emite la Entidad correspondiente para verificar la integridad del mismo, en donde constará cualquier modificación en caso de haberla.

  Lorenzetti menciona que "si se manda un correo electrónico firmado digitalmente, éste no puede abrirse y cambiarse su contenido sin afectar su vinculación con la firma certificada" añadiendo "si algo se altera, el certificado lo avisa"[17].
- *Presunción de prueba*: como expliqué en el no repudio, cualquier negación respecto al envió o recepción de un documento firmado digitalmente no será tomado en cuenta,

[16] http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf
[17] LORENZETTI Ricardo; *Comercio Electrónico*; Abeledo Perrot, Buenos Aires, Argentina; p. 82.

esto gracias a la intervención de la Entidad Certificadora, convirtiendo de esta manera a la firma en un medio probatorio, correspondiendo a quien niegue su validez, probarlo.

- *Presunción de obligatoriedad*: Al contratar por medios electrónicos con sustento legal de firma electrónica, las partes intervinientes se obligarán legalmente con la simple aceptación de ambas, siendo esta firma manifestación de la voluntad y requisito de existencia de todo contrato, quedando como único motivo de ilegalidad la incursión de cualquiera de los vicios del consentimiento (error, fuerza y dolo) tipificados en el Código Civil.

1.3 Elementos

Dentro de la presente investigación encontré a tratadistas que hablan sobre la presencia de ciertos elementos necesarios para la existencia plena de la firma digital, haciendo un pequeño barrido de lo ya explicado y enumerando puntos claves como el hecho de que la firma digital se la realiza por medios electrónicos, la cual vincula al firmante con el texto, sin que esta conste dentro del propio instrumento como sí sucede en la firma autógrafa, sino que va anexa, transformándose en algo inseparable; que, a pesar de ser éste medio suficiente para demostrar la autoría, no se cumple con la seguridad suficiente para darle valor jurídico, por eso es necesaria la inclusión de criptografía; que, la firma electrónica debe estar bajo estricto control de su titular, ya que él será el único responsable de su uso; y que, el receptor debe estar en capacidad de verificar la autoría, obviamente a través de una Entidad de Certificación. Como vemos, son puntos que ya los he tratado, pero siempre son necesarios su enunciación para así dejar clara toda parte interviniente en este proceso. Lo que realmente me admira y sorprende es el hecho de que dos escritores de distintos países, con distintas fechas de edición, describen estos elementos con palabras textuales, siendo idénticos el uno del otro, dando a pensar que su conexión intelectual es algo asombroso, es por esto que me permito citar a ambos:

"***Elemento objetivo-soporte:*** *En un sentido negativo, el soporte no es escrito, y no hay una elaboración manual del autor. En un sentido positivo, la firma es cualquier símbolo procedimiento de seguridad usado por una persona que incluye medios eléctricos, digitales, magnéticos, ópticos, electromagnéticos o similares. Puede advertirse entonces que la firma electrónica no necesariamente debe ir anexa a un documento, como ocurre en el caso de la firma ológrafa sobre un documento escrito.*

Elemento subjetivo: *Los símbolos asentados en medios electrónicos tienen un propósito específico: se hacen para identificar a la persona e indicar su aprobación del contenido de un mensaje electrónico.*

Con estos dos elementos puede haber firma electrónica, pero para que la ley asigne efectos de presunción, es decir, que cada vez que se vean esos signos se presuma que son de su autor, se requiere más seguridad.

Esfera de control del titular: *Siendo un elemento de imputación de autoría, es lógico que se requiera que esté bajo el control del titular, ya que sólo él es quien decide qué declaraciones de voluntad son suyas. Por ello, es necesario que la firma pertenezca únicamente a su titular y se encuentre bajo su control exclusivo.*

Derechos de verificación del receptor: *Se requiere que los sistemas utilizados puedan ser verificados por el receptor para asegurarse de la autoría.* "[18] y [19].

2. CRIPTOGRAFÍA

La criptografía no es un arte o ciencia que aparece conjuntamente con el nacimiento de las nuevas tecnologías, este es un método que se ha utilizado desde varios siglos atrás con la finalidad de proteger información de carácter confidencial de cualquier tipo de alteración, modificación o intercepción que pudiera existir, de esta manera se garantizaba la comunicación secreta entre dos personas o grupos.

Por lo general, ésta era usada durante campañas militares para enviar mensajes ocultos entre ejércitos aliados. Las tropas españolas de Felipe II utilizaron durante mucho tiempo un cifrado que consistía en un alfabeto de más de 500 símbolos que los matemáticos de este rey consideraban infranqueable. Cuando el matemático francés François Viète consiguió *criptoanalizar*, y por lo tanto descubrir aquel sistema para Enrique IV rey de Francia, el conocimiento mostrado por el rey francés acarreó una queja de la corte española ante del Papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. De igual forma, en la Grecia Antigua, se utilizó una herramienta llamada s*cytale*, la cual era un cilindro, de forma y dimensiones específicas, donde cada ejercito aliado tenía uno de ellos; alrededor de este objeto se enredaba una tira de cuero, de tal forma que el

[18] LORENZETTI Ricardo; *Comercio Electrónico*; Abeledo Perrot; 2001; Buenos Aires-Argentina; p. 80.
[19] PÁEZ Ribadeneira Juan José; *Manual de Firmas Electrónicas y Mensajes de Datos*; Corporación de Estudios y Publicaciones; 2005; Quito-Ecuador; p. 48.

cilindro quedará completamente cubierto y así escribir sobre éste el mensaje deseado. Finalmente se enviaba la tira de cuero con un mensaje aparentemente ilegible, llegando a su destino de manera segura.

Como se introdujo al principio de este capítulo, la criptografía consiste en la transformación de mensajes en textos aparentemente ilegibles en donde únicamente el emisor y receptor consiguen resolverlos a su forma original, alcanzando así que cualquier persona que no posea la clave le sea imposible descifrarlo, por lo general su creación es a través de algoritmos con los cuales se crean dos claves diferentes pero matemáticamente vinculadas entre sí, una de estas claves es utilizada para cifrar el mensaje o firmar digitalmente un documento, transformándolo en un texto ilegible, mientras que la segunda clave es utilizada para descifrar el mensaje o verificar la firma digital, transformando nuevamente al texto a su forma original. Este método se lo conoce como criptografía asimétrica de clave pública y es el de mayor uso en razón de las seguridades que brindan, pero no es el único, existe también la criptografía simétrica.

2.1 Características

Las características de la criptografía son muy similares a las funciones que tiene la firma electrónica, esto en razón de que la criptografía es necesaria para alcanzar los objetivos básicos de confidencialidad, integridad, autenticidad y no repudio que posee este tipo de firmas.

A continuación haré un pequeño recuento de estas características incluyendo una quinta la cual es propia de la criptografía.

- Conservar la *confidencialidad* de la información, es decir, el texto el cual ha sido enviado por medios telemáticos serán transformados en ilegibles para que únicamente emisor y receptor sean capaces de descifrar dicha información.
- Dar fe de la *autenticidad* tanto de emisor como receptor, asegurando de tal manera el vínculo inequívoco que debe existir entre emisor/receptor respecto del mensaje.
- Precautelar la *integridad* del mensaje, resguardando la información enviada de cualquier peligro de alteración o falsificación por terceras personas que pudiera existir dentro del lapso de transmisión.
- Garantizar el *no repudio* de la información, determinando irrefutablemente que las partes han enviado o recibido el mensaje.

- Permitir el *control de acceso* de información, garantizando así que solo usuarios autorizados puedan acceder al sistema de datos, teniendo disponibilidad de ellos cuando sean requeridos.

2.2 Criptografía Simétrica

También conocida como tradicional o de clave privada, la criptografía simétrica es aquel método de encriptación en el cual solamente existe una llave idéntica para cifrar y descifrar el mensaje, esto quiere decir que si deseamos utilizar a la criptografía simétrica como medio de autenticación, necesariamente la clave deberá ser conocida por el emisor y receptor, donde ambos tendrán que guardar el secreto.

La ventaja de este sistema radica en que su aplicación es mucho más rápida en comparación de la criptografía asimétrica, es decir, cuando existen textos muy extensos o grandes volúmenes de información al momento de cifrarlos mediante este método su aplicación se resolverá en poco tiempo.

La encriptación simétrica de mayor aplicación es *Data Encryption Standard* más conocida por su abreviatura *DES*, ésta fue desarrollada en los Estados Unidos en 1976 por la compañía de computación IBM; para su época este era un medio tan seguro que hasta fue usado por el gobierno estadounidense para proteger su información. Posterior a este sistema fueron apareciendo otros métodos como 3DES, Blowfish e IDEA, basando su peculiaridad en que poseían claves más extensas, pero igualmente descifrables en un tiempo relativamente mayor.

La rapidez del criptosistema simétrico consiste en la extensión del algoritmo de cifrado que utilizan (no pretendo extenderme en temas técnicos pero creo necesaria una explicación básica para mayor comprensión), por ejemplo, en el cifrado de DES se utiliza una clave de 56 Bits, *Bit* es el acrónimo de Binary Digit (digito binario), en el cual únicamente se utilizan dos de los números binarios (0 y 1), por lo cual si hacemos el cálculo matemático de 2 elevado a 56 nos da como resultado 72.057.594.037.927.936 claves posibles. Aparentemente es un número muy extenso pero el alto desarrollo de los sistemas de computación hace descifrable a este método en un mediano plazo de tiempo volviendo vulnerable a nuestra información.

Por lo tanto, teniendo un mecanismo donde existe una clave idéntica para cifrar y descifrar el mensaje de datos enviado, existen algunos problemas:

- *Acceso a la clave*; necesariamente ambas partes deben estar en conocimiento de la clave para poder enviar y recibir el mensaje, y lógicamente su envió no puede hacerse a través de un simple correo electrónico. La situación se dificulta, debiendo el remitente contactarse con el destinatario o viceversa, lo cual traba la celeridad del acto, ya que deben recurrir a llamadas telefónicas o encuentros personales, pero ¿qué pasaría si están en distintos países? ¿O su único referente es el correo electrónico de una página Web? Es por esto que se pierde la facilidad que por esencia nos brinda la firma digital.
- *Secreto*; Al ser la clave un dato compartido entre ambas partes, la seguridad de sus mensajes radica en la confianza y sigilo que puedan tener los usuarios para que la información no se vea alterada por terceras personas. *El secreto mejor guardado es aquel que no se cuenta.*
- *Límite de usuarios*; esto va vinculado con el literal anterior; mientras más personas conozcan la clave, más vulnerable es esta. Su uso reside en la confianza de las partes.

2.3 Criptografía Asimétrica

A fin de que la firma electrónica cumpla con todas sus funciones, es necesaria la aplicación de criptografía asimétrica o también llamada de clave pública. Esta clase de criptosistema consiste en que cada usuario tenga un par de claves, una pública la cual podrá ser conocida por todos, y una privada, en donde el propietario deberá guardarla y él será el único que la posea sin que necesariamente la conozca, ya que esta clave privada se podrá encontrar dentro de un dispositivo de memoria individual, dentro del propio ordenador o mejor aún, se podrá acceder a través de un dispositivo de lectura de huella digital, los cuales en la actualidad ya vienen incorporados en algunas computadoras portátiles o como hardware adicional.

Este método fue creado como solución a los problemas que existen dentro de la criptografía simétrica, ya que los riesgos por el intercambio de claves eran altos, basándose únicamente en la confianza de uno a otro. Aquí únicamente se requiere obtener la clave pública del destinatario y enviar el documento firmado.

El cifrado asimétrico tiene sus bases de seguridad en la utilización de números primos (números únicamente divisibles por si mismos y por 1) en donde su encriptación se da aplicando lo que matemáticamente se conoce como *función trampa* (función que se aplica en un solo sentido) esto las convierte en fáciles de cifrar pero difíciles de descifrar, es

decir, multiplicar dos números primos grandes es sencillo, mientras que encontrar los componentes del resultado es excesivamente difícil, donde además existe una *trampa* que consiste en un dato adicional desconocido, volviéndolo mas complicado aun si se llegara a conocer uno de los dos números.

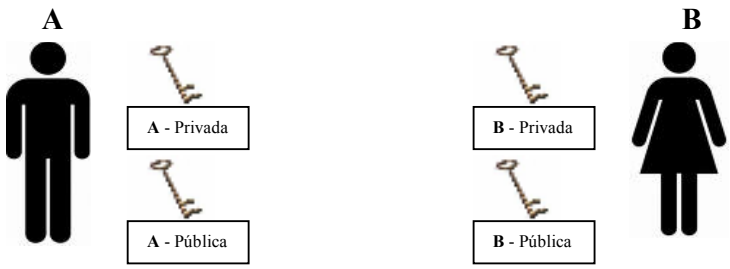
"El criptosistema (o familia de funciones) de cifrado asimétrico o de clave pública, utiliza un par de claves. Una es pública y la otra es secreta o privada. Cada clave efectúa una transformación unívoca sobre el mensaje y es función inversa de la otra, de modo que cada par de claves puede descifrar sólo lo que su par correspondiente cifró."[20]

Como vimos, cada usuario estará en posesión de dos claves, publica y privada, la primera será de conocimiento general, mientras que la otra se mantendrá en secreto, ambas claves son usadas para cifrar o descifrar un mensaje, por ejemplo, si tenemos dos sujetos (A y B), donde A quiere enviar un mensaje firmado digitalmente a B, A deberá utilizar la clave pública de B (Kpu) para encriptar el mensaje que ha escrito y lo enviará a B quien mediante su clave privada (Kpr), será el único capaz de descifrar dicho mensaje, pudiendo verificar la identidad del firmante mediante la Kpu del emisor, es decir de A. Por lo tanto, el mensaje fue encriptado por A con la Kpu de B y fue descifrado por B con su propia clave privada.

Lo mismo sucederá a la inversa, en el caso de que A desee enviar un documento digitalmente firmado, lo puede encriptar con su Kpr, para que B lo descencripte con la Kpu de A.

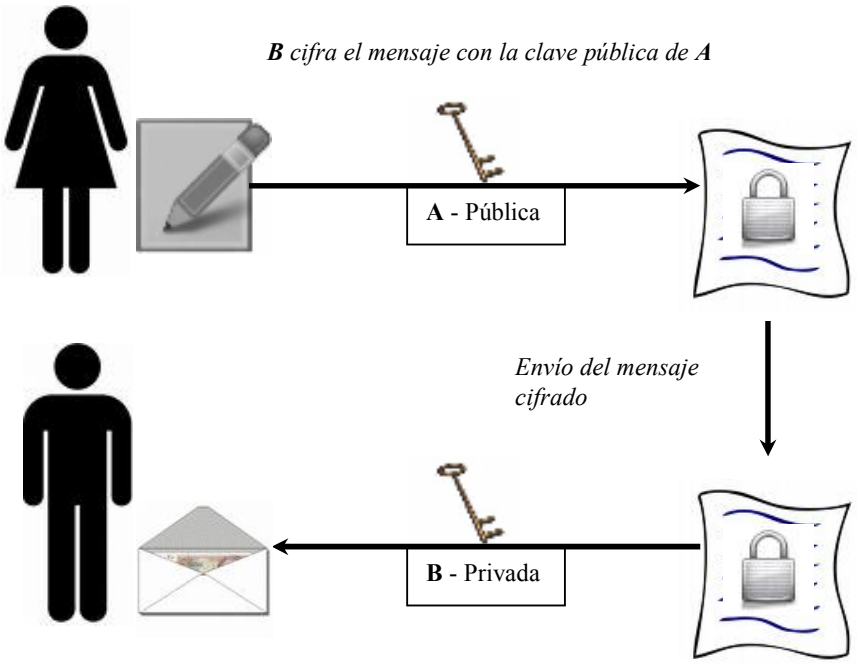
Para mayor entendimiento a continuación se grafica lo explicado:

- ***Gráfico 1:***



[20] SARRA, Andrea Viviana; *Comercio Electrónico*… p. 60

- ***Gráfico 2:*** (Proceso)



2.4 Función Hash

Es necesario enfatizar en el hecho de que los algoritmos usados en la criptografía asimétrica de llave pública son significativamente más lentos que los de encriptación simétrica. Por tal razón se utiliza varias encriptaciones las cuales aceleran el proceso, estableciendo la eficacia requerida.

Este cifrado adicional se lo conoce como función hash (*hash funtion*), cuyo objetivo consiste en obtener un resumen o digesto del texto original. Al hash se lo puede establecer como "un número que se obtiene haciendo una operación matemática sobre todos los datos del mensaje, de tal manera que si el mensaje variara aunque sea en un *bit*, el *hash* sería totalmente diferente"[21].

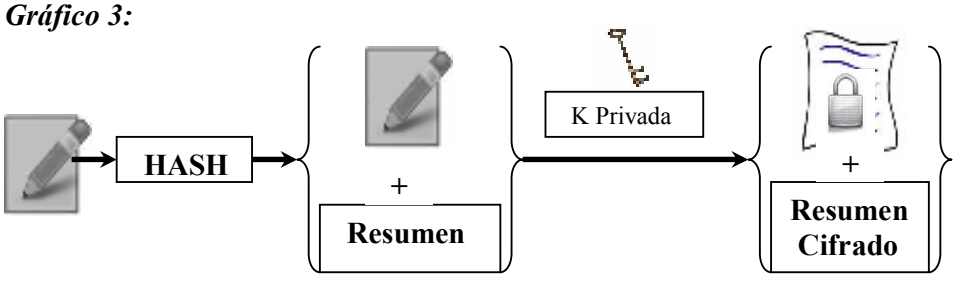
Esta función se caracteriza por lo siguiente:

- *Longitud fija*; sin importar la extensión del documento al que se aplique, el resumen que se obtiene no será mayor a 16 bits.
- *Irreversible*; Una vez que se utiliza la función hash sobre un texto, se vuelve imposible adquirir el texto original partiendo del digesto. Es por esto que se diferencia de los

[21] HOCSMAN Heriberto Simón; *Negocios en Internet*; Ed. Astrea 2005; p. 365

sistemas de compresión comunes, como ZIP, RAR, CAB, etc… los cuales cumplen con el objetivo de reducir el tamaño del texto para posteriormente devolverlo a su estado original.

- *Único*; el resumen hash siempre será unívoco del texto que se aplica, utilizada la función sobre un mensaje de datos, cualquier variación ulterior que se realice sobre el mismo, por insignificante que esta sea, arrojará un hash completamente distinto, garantizando la siguiente característica.
- *Medio de comprobación*; cuando el emisor envía el documento firmado digitalmente, lo hace conjuntamente con el hash respectivo, debiendo el receptor aplicar la función hash sobre el documento que ha recibido para verificar que ambos digestos, el que él efectuó y el que recibió, son exactamente iguales. Se determina de tal manera que no ha existido alteración alguna respecto del mensaje recibido con el documento original, ya que si habría existido interceptación los hash hubieran sido distintos.
- *Celeridad en el cifrado*; como se mencionó, los algoritmos de encriptación asimétrica son lentos y al aplicarlos en documentos extensos podría tomar tiempo, es por esta razón que el emisor se encuentra facultado de firmar el resumen hash, agilitando tiempo de encriptación sin alterar la seguridad ya que a pesar de envíe el mensaje original por la red, el digesto el cual garantiza que no se altera el documento, va encriptado. Por lo tanto, el receptor del mensaje usará la función hash sobre el documento que ha recibido para compararlo con el digesto anexado posterior a la descencriptación del mismo, verificando de tal manera si se ha modificado o no el documento original.
- ***Gráfico 3:***



Destacando las ventajas de esta función, Froomkin realiza una enumeración tripartita: "en primer lugar, las funciones hash son públicas, por lo que cualquier personal puede repetir el cálculo para determinar si el documento original fue modificado. En segundo término, es una función de sentido único que permite confirmar que el hash del documento ha variado,

pero no permite recrearlo. En tercer lugar, es prácticamente imposible que dos documentos diferentes produzcan la misma función hash."[22]

3. FUNCIONAMIENTO

Dentro del proceso de firma digital, como es claro, existen dos sujetos involucrados, por una parte el signatario quien es una persona natural o jurídica, la cual firma el documento; y por otra, el receptor que al igual podrá ser una persona natural o jurídica que recibe el mensaje de datos firmado.

Cada uno de estos sujetos posee dos elementos fundamentales para firma y recibir el documento:

El signatario firmará el documento a través de:

- *Datos de creación de firma*; los cuales consisten en códigos o claves criptográficas privadas que el signatario utiliza para crear la firma electrónica.
- *Dispositivo de creación de firma*; es un programa informático o software que aplica los datos de creación de firma (consiste en una clave privada utilizada para encriptar el mensaje.)

El receptor a su vez recibe el documento por medio de:

- *Datos de verificación de firma*; son los datos (códigos o claves criptográficas públicas) que se utilizan para verificar la firma electrónica. Consiste en una clave pública utilizada para desencriptar el mensaje.
- *Dispositivo de verificación de firma*; Al igual que el dispositivo de creación de firma, el de verificación es una aplicación informática o software que utiliza los datos de verificación de firma o clave pública y se encarga de detectar cualquier alteración o modificación de los datos firmados.

Con esta explicación y habiendo ya analizado cada uno de los componentes que se encuentran inmersos en la aplicación de la firma electrónica, a continuación se establece paso a paso el funcionamiento de ésta, ejemplificando el supuesto de que **A** envía a **B** un mensaje de datos:

1. El emisor (**A**) una vez que ha realizado el mensaje de datos que desea enviar, utiliza sobre éste la función hash obteniendo un resumen de longitud fija e incomprensible.

[22] FROOMKIN; *The Essentials role of trusted third parties in Electronic commerce*; www.law.miami.edu/~froomkin/articles/trusted1.htm

2. **A** se valdrá de su clave privada para encriptar el mensaje original y el digesto (o únicamente el digesto si así él lo desea), transformándolos en textos ilegibles, asegurando la confidencialidad del envió. La firma electrónica quedará representada por el mensaje cifrado.
3. **A** envía cifrados tanto el mensaje como el digesto (o solo cifrado el digesto) a **B.**
4. Acaecida la recepción, **B** utilizará la clave pública de **A** (la cual es de conocimiento general) a fin de descifrar los datos encriptados; también conocida como *dispositivo de verificación de firma*.
5. **B** utilizará la función hash sobre el mensaje de datos que ha recibido obteniendo su propio digesto o resumen, para realizar la comparación respectiva entre su hash y el que le fue enviado.
6. De no existir diferencia entre ambos digestos, el proceso habría concluido exitosamente entre **A** y **B** ya que de haber existido una alteración mínima en el mensaje original, habría dado como resultado un digesto diferente entre emisor y receptor.

De esta manera se ha conservando las características de *confidencialidad* por medio del cifrado, *autenticidad* ya que la procedencia quedó determinada a través de la firma, *integridad* en razón de que los dos resúmenes fueron exactos y el *no repudio* por cuanto la clave privada es de uso y responsabilidad exclusiva del emisor; cumpliendo así con los elementos necesarios para la autenticación de un mensaje de datos enviado por medios informáticos.

Es necesario establecer que al efectuar este procedimiento mediante claves creadas por el propio firmante, no existiría el reconocimiento legal necesario ni la seguridad absoluta requerida, es por esto que las firmas electrónicas deben ser certificadas por entidades habilitas para prestar servicios de certificación de información y demás servicios relacionados, con las cuales existirá un nexo contractual entre la entidad y el usuario atribuyendo los efectos jurídicos a las relaciones posteriores que realicen los usuarios, teniendo derechos y obligaciones los cuales se encuentran debidamente sancionados en nuestra legislación.

Como lo menciona Devoto "La función básica de estos sujetos es la de emitir certificados de clave pública, certificados que vincularán a una persona con una clave pública."[23]

[23] DEVOTO Mauricio; *Comercio Electrónico y Firma Digital*; Ed. La Ley, 2001; p. 209

CAPÍTULO III
CERTIFICADOS ELECTRÓNICOS Y ENTIDADES HABILITADAS

Hasta este punto ya contamos con todos los medios para determinar la identidad de los sujetos involucrados en el envío de un mensaje de datos, tenemos vía segura de transmisión y gozamos además de la confidencialidad y seguridad de la inalterabilidad de nuestros documentos, pero falta un elemento de suma importancia en la relación: la confianza y certeza de que el sujeto con quien estamos tratando es en verdad quien dice ser.

Dentro de un grupo cerrado, reducido o en una misma empresa, donde nuestros actos se efectúan con personas conocidas y de confianza, por cuanto utilizamos sistemas criptográficos simétricos o asimétricos sin valor monetario alguno, como el PGP[24][25] (*Pretty Good Privacy*), cuyo grado de seguridad es alto, el sistema de transmisión funcionaría sin complicaciones mayores. El problema radica en los negocios de relevancia jurídica entre dos personas que no se conocen.

¿Como garantizamos el vínculo entre una firma electrónica y una persona? ¿De qué nos valemos para determinar el valor legal de la obligación contraída? ¿Qué tercero de confianza avala nuestros actos jurídicos con individuos desconocidos? Todas estas interrogantes se resuelven con la existencia de un tercero fiscalizador, un tercero jurídicamente constituido y controlado generalmente por el Gobierno Central del Estado, un tercero que nos brinda confianza frente a una relación jurídica constituida con un usuario ignoto.

Es por estas razones que para realizar el envío-recepción de mensajes de datos mediante sistemas de autenticación de autoría con reconocimiento legal a través de redes abiertas, es ineludible la existencia de una esfera procesal la cual enmarque todo aquello vinculante

[24] Programa desarrollado por Phil Zimmermann (1991) cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

al funcionamiento, esto se lo conoce como infraestructura de clave pública (*Infraestructura PKI*), donde se engloba a los usuarios del cosmos transaccional informático, a las *Entidades de Certificación de Información y Servicios Relacionados* y a las políticas de operación.

Se puede entender como Infraestructura de Clave Pública al conjunto de software, hardware, procedimientos y políticas generales de Firma Electrónica, cuyo objetivo es gestionar la certificación electrónica y servicios relacionados.

Actualmente dicha estructura se constituye como la más completa y funcional; tanto es así, que es considerada la de mayor uso y difusión mundial para la ejecución del comercio electrónico seguro.

Respecto a este tema, en el año 2003, dentro de la legislación ecuatoriana mediante Resolución del CONATEL (*584-23-CONATEL-2003*), se determinaba a la Infraestructura PKI como elemento gestor para el proceso de firma electrónica. Como es lógico, la normativa legal dentro del ámbito informático no puede estar supedita de manera excluyente a un único proceso de transmisión de datos, por cuanto el avance tecnológico es extremadamente acelerado. Por esta razón, cinco años después nuestros representantes han declarado la improcedencia de dicha norma, dando como resultado su derogación, a fin de dejar abierta la posibilidad de implementar nuevos métodos técnicos que puedan surgir en el futuro, evitando el desuso de la ley.

La derogación que se acaba de mencionar (*Res. 478-20-CONATEL-2008*) instituye un hecho digno de razonamiento y consideración por parte de nosotros como gobernados, ya que no supone la acertada ampliación legislativa, por el contrario, es el resultado de un error por parte de la Administración Pública, la cual ocasionó un retraso considerable en el funcionamiento de tres compañías privadas como Entidades de Certificación (*SISTECION S.A., ESDINAMICO CIA. LTDA. y ECUACERT S.A.)* y por consiguiente la dilación comunitaria en el aprovechamiento de los beneficios que nos brinda esta tecnología, dejando además la calidad de primitiva e inaplicable a cualquier doctrina ecuatoriana que haya versado sobre el tema.

Como ya sabemos, nuestra normativa en comercio electrónico se encuentra vigente desde el 2002, pero desde entonces sus vacíos y falencias no fueron considerados por los legisladores, es por esto que el CONATEL como entidad de regulación, por ingenuidad, buena fe o descuido, decidió emitir resoluciones en las cuales constaban disposiciones necesarias para el funcionamiento de la firma electrónica. Dentro de éstas resoluciones se

incluían figuras como *Títulto Habilitante, modelos, permisos de funcionamiento…*, que eran nuevas y distintas a las ya constantes en la Ley 67.

Lamentablemente esto se hizo sin considerar el *principio de restricción de contenido* normado en el artículo 67 del Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva (ERJAFE), el cual dice que "Las resoluciones administrativas de carácter particular (*resoluciones del CONATEL*) no podrán vulnerar lo establecido en una disposición de carácter general (*Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*), aún cuando aquellas tengan grado igual o superior a éstas", lo cual sumado al artículo 93 del mismo cuerpo legal que dispone que "Cualquier acto administrativo expedido por los órganos y entidades sujetas a este estatuto (*CONATEL forma parte de él*) deberá ser extinguido cuando se encuentre que dicho acto contiene vicios que no pueden ser convalidados o subsanados." Esto derivó en la necesidad de derogar las dos resoluciones del CONATEL (*324-17-2006 y 454-19-2006*) en las cuales constaban definiciones y procedimientos para la creación de Entidades de Certificación; disposiciones que fueron aplicadas y cumplidas a cabalidad por las precitadas compañías, a tal punto que ya existieron resoluciones aprobatorias por parte del CONATEL para su permiso y registro (*456-19-06, 457-19-06 y 458-19-06*), pero en razón de que la normativa a la que ellas se rigieron era improcedente e ineficaz, también se debió derogar sus permisos.

Analizando este suceso, se ratifica la importancia de dos aspectos básicos; por una parte la capacitación y sapiencia jurídica que requieren nuestros funcionarios públicos para la correcta ejecución de sus funciones, y por otra, la preocupación y seguimiento que se debe dar a la normativa naciente por parte del Legislativo, a fin de que se pueda cubrir y subsanar el surgimiento de posibles lagunas legales que afecten su validez y aplicabilidad. Si no enmendamos estos factores, penosamente este hecho pasará de ser aislado a cotidiano, donde el único perjudicado será el Pueblo, el cual vivirá en la incertidumbre constante del posible daño que le causará cualquier desatino administrativo público.

1. CERTIFICADOS DE FIRMA ELECTRÓNICA

"Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad."[25]

Así mismo, la Directiva 1999/93 del Parlamento Europeo y su Consejo define estos certificados como "la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de esta."[26]

Como ya se mencionó anteriormente, nuestro principal problema en las actividades comerciales con otros internautas radica en la vinculación del par de claves con la persona física, necesitando un resguardo respecto al nexo sujeto-firma. Es por esto la existencia de Certificados de Firma Electrónica, estos documentos (igualmente digitales) ratifican fehacientemente la pertenencia de la firma electrónica al individuo en cuestión, dejando de lado cualquier posible falsificación o suplantación de identidad que podría existir en el acto o contrato.

A estos certificados se los puede establecer como testimonios intachables que validan la pertenencia e identidad de una persona natural o jurídica respecto a determinada firma electrónica.

1.1 Contenido del Certificado

La importancia de estos certificados es tan alta que fácilmente los podríamos comparar con nuestros documentos de identificación personal, los cuales nos validan en relaciones interpersonales como la celebración de contratos, permitiendo la adquisición de derechos y obligaciones, constituyendo garantía suficiente de probidad jurídica como sujetos de derecho.

Considerando el reconocimiento y valor legal que poseen los certificados electrónicos, es necesario determinar cuales son los requisitos mínimos que deben contener estos documentos:

- *Identificación de la entidad de certificación de información*; mediante este dato, además de determinar la institución que controla la actividad jurídica del otro usuario,

[25] Art. 20; *Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos (*Ley 67*)*
[26] HERRMANN FERNÁNDEZ Patricia; *Comercio Electrónico;* Ed. Universidad Técnica Particular de Loja; 2007; p. 124

contamos con el nombre del garante que da fe de la veracidad del sujeto y de su firma, quien además será legalmente responsable en caso de que los datos expedidos en el certificado hayan sido falsos y por esto se nos haya ocasionado algún perjuicio.

- *Domicilio legal de la entidad*; de tal manera se establece el domicilio jurídico de la entidad de certificación, validando su constitución legal.
- *Datos generales del titular*; titular es aquel sujeto con el cual se ha entablado la relación. Estos datos nos ratificarán la identidad del usuario permitiendo conjuntamente su ubicación física en caso de ser requerida.
- *Fecha de emisión y expiración*; Por medio de estas fechas se establece el periodo durante el cual el suscriptor puede firmar documentos digitales utilizando su par de claves. La duración del certificado será establecido dentro del contrato del titular con la entidad de certificación, en caso de no haberse estipulado, el plazo de validez será de dos años contados a partir de que fueron expedidos. Cabe mencionar que dentro de este periodo puede existir la revocación o suspensión del certificado[27].

  La suspensión principalmente podrá darse por disposición expresa y motivada de la Autoridad Reguladora (CONATEL); por falsedad en los datos del suscriptor o por incumplimiento contractual por parte del titular de la firma; esta suspensión será de carácter temporal y deberá ser levantada una vez superadas las causales o a través de una resolución del CONATEL.

  En el segundo caso, la motivación para revocar un certificado de firma electrónica radica en los supuestos de que la entidad de certificación haya cesado sus funciones y los certificados vigentes no hayan sido asumidos por otra entidad, o en el caso de existir la quiebra técnica de la entidad de certificación, habiendo sido declarada judicialmente.

  Ahora bien, en el caso de que se produzca cualquiera de las limitaciones antes citadas, será obligación de la Entidad de Certificación de Información y Servicios Relacionados contar con mecanismos de ejecución inmediata para la cancelación de certificados, permitir el acceso público, dentro de su página Web, a listados de actualización permanente, en los cuales consten los certificados extintos, suspendidos y revocados, los cuales serán proporcionados por mecanismos automáticos cuya verificación deberá ser en tiempo real y notificar inmediatamente de la revocación a sus usuarios, dentro de las 24 horas posteriores[28].

[27] Art. 25 y 26; *Ley 67*
[28] Anexo de la Resolución 477-20-CONATEL-2008; *Art.3 # 5, Art.4 #8, 14 y 16.*

Queda así demostrado, la seguridad que los legisladores han decidido brindar a los usuarios, otorgando los medios necesarios para que los sujetos que intervienen en el acto puedan verificar la legalidad y vigencia de la firma electrónica de cada uno de ellos; hecho que se basa en lo dispuesto en el artículo 55 de la Ley Modelo de la CNUDMI referente a Firmas Electrónicas, el cual versa "La firma numérica correspondiente a un mensaje, ya sea creada por el tenedor de un par de claves para autenticar un mensaje o por una entidad certificadora para autenticar su certificado, deberá contener por lo general un sello cronológico fiable para que el verificador pueda determinar con certeza si la firma numérica fue creada durante el "período de validez" indicado en el certificado, que es una condición para poder verificar una firma numérica."

- *Número único de serie del certificado*; a través de esto se crea la individualidad de cada certificado, volviéndose heterogéneo respecto de los demás, facilitando así su búsqueda. A este número se lo conoce como "identificador exclusivo" y constituye obligación de la Entidad de Certificación, emitirlos con esta distinción. De igual forma, este requisito se encuentra reglado dentro de las Políticas de Seguridad que debe contar la Entidad de Certificación (*Art. 3 # 8 Res. 477-20-CONATEL-2008*).
- *Firma electrónica de la entidad*; por medio de esta se garantizará los principios de confidencialidad, integridad, autenticidad y no repudio de la información recibida por parte de la entidad de certificación, donde además quedará constancia de la veracidad del certificado recibido dejando como responsable a la propia entidad en caso de cualquier alteración o falsedad.
- *Limitaciones del certificado*; dentro de este último campo, la entidad dejará constancia expresa de que la información inmersa dentro del certificado podrá ser utilizada como medio ratificatorio de autoría y que el texto que envuelve al mensaje de datos será responsabilidad exclusiva del emisor; pudiendo además incluir otras limitaciones dependiendo de cada legislación.

Finalmente podríamos definir tres funciones fundamentales que cumple un certificado de firma electrónica:

1. Identificar a una persona natural o jurídica y vincularla con su firma digital.
2. Identificar las responsabilidades asociadas tanto de la Entidad de Certificación como del usuario.

3. Garantizar por parte de un tercero de confianza la pertenencia de un sujeto respecto a una firma electrónica y su vigencia de uso.

1.2 Certificados Emitidos en el Extranjero

Con la aplicación de los elementos anteriores, nace una negociación informática legalmente estable y reconocida dentro de un mismo territorio, pero la tendencia del comercio viene a ser internacional, en donde se derriban fronteras y los lazos productivos se dan entre sujetos de nacionalidad dispar.

Es cierto, como lo hemos estado analizando, que la tipificación del tema tiene carácter mundial donde la batuta la llevan las organizaciones internacionales como la ONU, CAN, Unión Europea entre las mas destacadas, las cuales envuelven congregaciones de estados; es por esto que acertadamente se ha incluido el reconocimiento de certificados de firma electrónica emitidos en el extranjero, tal es el caso de la UNCITRAL (CNUDMI), la cual menciona en su artículo 58 que

> "… El reconocimiento de certificados extranjeros se realiza generalmente mediante un método denominado "certificación cruzada". En tales casos es necesario que entidades certificadoras sustancialmente equivalentes (o entidades certificadoras dispuestas a asumir ciertos riesgos con respecto a los certificados emitidos por otras entidades certificadoras) reconozcan mutuamente los servicios prestados, de forma que los respectivos usuarios puedan comunicarse entre ellos de manera más eficaz y con mayor confianza en la fiabilidad de los certificados que se emitan."

de igual manera lo realiza la Comunidad Europea determinando en su séptimo artículo dictado por la Directiva 1999/93/CE, que "los Estados miembros velarán por que los certificados expedidos al público como certificados reconocidos por un proveedor de servicios de certificación establecido en un tercer país, sean reconocidos como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad…"[29] además de esto, la UE establece ciertos requisitos que el tercer país deberá cumplir:

[29] Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:ES:HTML

- que el proveedor de servicios de certificación cumpla los requisitos establecidos en la presente Directiva y haya sido acreditado en el marco de un sistema voluntario de acreditación establecido en un Estado miembro;
- que un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones de la presente Directiva, avale el certificado;
- que el certificado o el proveedor de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

Con estos antecedentes, nuestra legislación ha procurado respetar estas disposiciones, declarando que los certificados emitidos en el extranjero tendrán el mismo valor legal que aquellos expedidos en el Ecuador. Este reconocimiento se puede dar por dos vías:
Primero, mediante solicitud de la entidad extranjera para su Acreditación en el país, previo a demostrar su reconocimiento legal de los servicios prestados en el extranjero. Es necesario mencionar que una vez adquirida la Acreditación legal por parte de la Entidad de Certificación Extranjera, ésta gozará de la calidad de entidad de certificación acreditada en el país, teniendo los mismos derechos y obligaciones que cualquier certificadora nacional.
Por otra parte, los certificados extranjeros también adquirirán validez jurídica en el país a través de una revalidación por parte de una Entidad de Certificación acreditada ante el CONATEL, la cual deberá comprobar la fiabilidad, tanto del certificado como de la entidad emisora. Estos hechos se encuentran debidamente tipificados en la Ley de Comercio Electrónico y Reforma al Reglamento General, en los artículos 28 y 2 respectivamente.
Es necesario destacar, que igualmente estos certificados tendrán carácter probatorio una vez validados.

2. ENTIDADES DE CERTIFICACIÓN

Ahora bien, ya demostrada la necesidad de los certificados de firma electrónica como medio para brindar seguridad y confianza a los usuarios en razón del auge del comercio electrónico, nacen las Entidades de Certificación, las cuales son sujetos, públicos o privados, encargadas de generar confianza en las transacciones comerciales por medios electrónicos y que se encuentran bajo el control de un ente público.

La Ley de Comercio Electrónico (Art. 28) las define como "empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República."

Como se desprende de lo citado, la función básica de las Entidades de Certificación radica en la emisión de certificados, pero a más de esto, se encuentran facultados de prestar servicios relacionados, dentro de los principales se encuentran:

- receptar la solicitud de emisión de un certificado electrónico;
- verificar y autenticar los datos que le entrega quien realiza la solicitud;
- generar las claves correspondientes para el certificado;
- grabar estas claves en un dispositivo físico, (token o tarjeta inteligente);
- administrar y mantener el sistema de claves, su estado, validez, y referencias; y
- realizar auditorias periódicas.

Es decir, estas entidades se encargan del funcionamiento y control global de las negociaciones telemáticas, otorgando la seguridad entre sus usuarios, haciendo posible el valor jurídico que éstas merecen.

Reyes Krafft acertadamente puntualiza sus actividades como "la generación, producción, distribución, control, seguimiento y destrucción de las llaves públicas o privadas asociadas con los certificados de llave pública."[30]

Si bien es cierto, las Entidades de Certificación nacen con la aparición de las nuevas tecnologías y el establecimiento de actos jurídicos y de comercio que se dan a través de ellas, pero sus raíces vienen de una figura preexistente. A pesar de no existir exactitud de funciones, su similitud es evidente con los Notarios Públicos, ya que ambos dan fe, legalmente reconocida, respecto a determinados hechos y su relevancia es pareja en razón de que los dos son importantes en sectores productivos porque brindan certeza sobre el autor y contenido de documentos; brindan seguridad jurídica y además se constituyen en fedatarios, donde la entidad de certificación específicamente es un tercero disipador de conflictos porque conoce la autoría de los mensajes de datos. "La función primordial de esta figura es dar fe que las transacciones electrónicas de datos se han producido, y constituirse como una tercera parte confiable que acredita un vínculo entre una persona y

[30] REYES KRAFFT Alfredo; *La Firma Electrónica y las Entidades…*; p. 192

una clave pública, pudiendo considerarse que actúa como una especie de 'notario electrónico'."[31]

Ahora bien, habiendo puntualizado la facultad que tienen los sujetos públicos y privados para constituirse en Entidades de Certificación, dentro del campo estatal, el CONATEL mediante Resolución 481-20-CONATEL-2008, con fecha 8 de octubre de 2008, otorgó al Banco Central del Ecuador la acreditación como Entidad de Certificación de Información y Servicios Relacionados, constituyéndose en el primer ente público que recibe esta facultad por parte del Estado ecuatoriano.[32]

2.1 Terceros Vinculados

En razón de las diversas obligaciones que posee una Entidad de Certificación, la legislación ha prevenido la facultad para delegar a una segunda entidad, de menor rango, a fin de que cumpla con funciones específicas y aliviane su carga de trabajo. A estas entidades subsidiarias se las conoce como *Terceros Vinculados*, cuyas características son:

- Tienen jerarquía menor a las Entidades de Certificación (EC);
- Es una intermediadora entre el usuario y la EC;
- Sólo se encargan de la fase de recepción de datos, verificación y entrega de los certificados emitidos por la EC al cliente;
- No tienen control sobre los algoritmos de generación, su seguridad ni sobre la administración de los certificados.

La figura de Tercero Vinculado se la entiende como un tercero acreditado en el CONATEL, relacionado contractual y legalmente con una entidad de certificación de información acreditada, la cual está autorizada para representarla legalmente y prestar servicios de certificación de información y relacionados, a nombre o en representación de la misma.

Dentro de nuestra legislación (Art. 33 Ley de Comercio Electrónico), se faculta a las Entidades de Certificación la posibilidad de brindar los servicios de certificación, de forma total o parcial, por medio de un tercero, previa a demostrar el vínculo contractual que existe entre ambas. De manera complementaria, la Reforma al Reglamento General de la Ley 67 (*Ley de Comercio Electrónico*) establece que su vida jurídica será igual al plazo de

[31] HOCSMAN Heriberto Simón; *Negocios en Internet*; Ed. Astrea 2005; p. 373

[32] http://www.conatel.gov.ec/site_conatel/index.php?option=com_content&view=article&id=371:resoluciones-octubre-diciembre-2008&catid=134:resoluciones-2008&Itemid=201

duración de la relación contractual con la Entidad de Certificación, adquiriendo esta última la responsabilidad respecto de los servicios prestados.

Sus funciones principales consistirán en la recopilación y custodia de información y documentos de soporte requeridos para la emisión de firmas electrónicas y certificados de firma electrónica; y, la instalación y soporte de aplicaciones relacionadas con el uso y verificación de firmas electrónicas y certificados de firma electrónica.

De esta manera podemos concluir en que el rol que debe cumplir la Entidad de Certificación versa en la ejecución de todas las fases del proceso e incluso administra y expide los certificados y los algoritmos de generación.

Dentro de la ejecución de la fase administrativa, se anida dos obligaciones puntuales de suma importancia; la primera consiste en mantener sistemas de respaldo de la información relativa a los certificados; en la mayoría de normativa internacional a esto se lo conoce como "repositorio", el cual consiste en una base de datos abierta al público, donde figura el historial de los certificados de firma electrónica que han sido expedidos por parte de la entidad, permitiendo a los usuarios la verificación de vigencia y validez de las firmas electrónicas. "Para que una clave pública y su correspondencia con un firmante específico se pueda utilizar fácilmente en una verificación, el certificado debe publicarse en un repositorio o difundirse por otros medios. Normalmente, los repositorios son bases de datos electrónicas de certificados y de otro tipo de información a los que se puede acceder y que pueden utilizarse para verificar firmas numéricas."[33]

En segundo lugar, se encuentra el deber de proteger los datos personales obtenidos directa o indirectamente del uso o transmisión de mensajes de datos.

En el artículo noveno de la Ley de Comercio Electrónico, estipula además que "La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.", de esta manera queda establecido el derecho a la reserva que tiene cada individuo respecto a su correspondencia, siendo además responsabilidad exclusiva del titular, el contenido de los mensajes de datos que este haya enviado, recayendo sobre el suscriptor la obligación de afrontar los cargos legales en caso de ser descubierto información enviada que atente contra las leyes o la seguridad nacional.

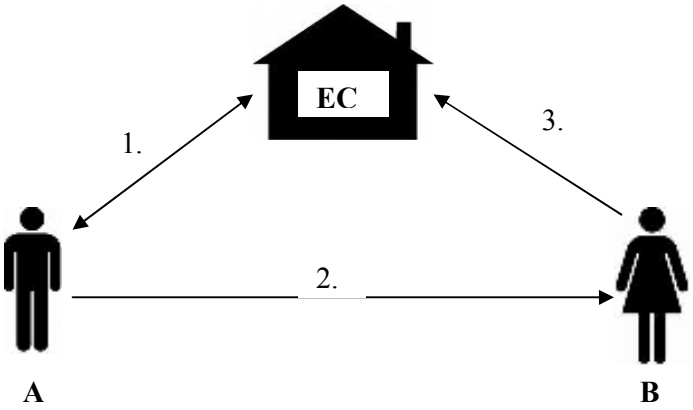
[33] CNUDMI; *Ley Modelo…*; Art. 56; http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

"Los autores J. Dianne Brinson y Mark Radcliffe manifiestan que en la mayoría de las jurisdicciones de los Estados Unidos y en el mundo se reconoce el derecho de todo individuo a tener privacidad. Pero cuando esa privacidad se transmite a una entidad de certificación de firmas electrónicas, esta última debe proteger los datos personales del titular. Pero en caso de que no se dé la correspondiente protección, el titular podrá tomar medidas legales en caso de que la entidad de certificación haya dejado escapar información de los datos personales."[34] Es por esta razón que el legislador ecuatoriano decretó que las entidades de certificación serán responsables hasta por culpa leve y responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad (Ley Comercio Electrónico Art. 31).

2.2 Emisión de Certificados

Una vez definidas las Entidades de Certificación y los Terceros Vinculados, a continuación se grafica la actividad práctica de emisión de certificados de firma electrónica que cumplen ambas; en el primer caso (*gráfico 4*) se establece como único ente a la Entidad de Certificación (**EC**), mientras en el segundo (*gráfico 5*) aparece la intervención del Tercero Vinculado (**3V**).

- ***Gráfico 4*:**

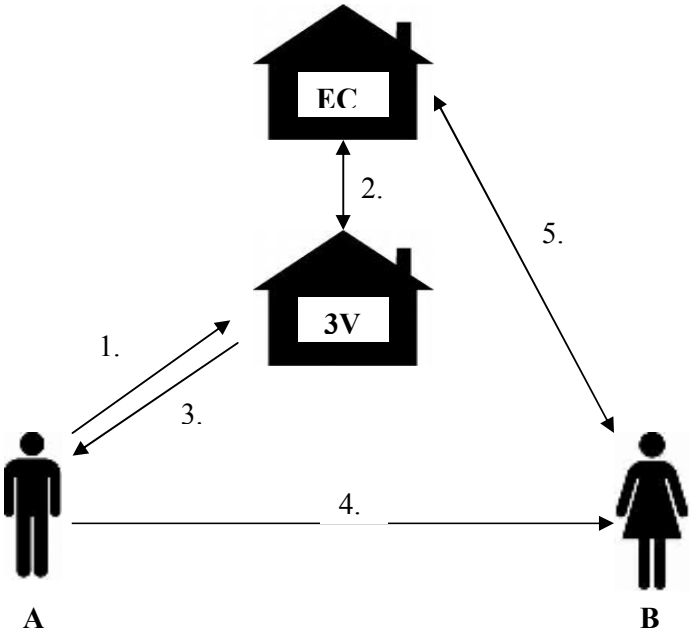


1. **A**, una vez elaborado el mensaje de datos que desea enviar, solicitará a la Entidad de Certificación que se le expida una certificación de firma electrónica. Inmediatamente **EC** verificará la identidad de A y emitirá el certificado a nombre del titular con su clave pública.

[34] HERRMANN FERNÁNDEZ Patricia; *Comercio Electrónico…*; p. 141

2. **A** encriptará el mensaje de datos con su clave pública, lo cual dará como resultado una firma electrónica, la cual será enviada conjuntamente con el certificado a **B**, donde este último descifrará la firma electrónica a través de la clave pública de **A**, obteniendo el mensaje original.
3. Opcionalmente **B**, para su mayor seguridad, ingresará al sistema de respaldo de información relativa a los certificados (repositorio) de la **EC**, para verificar la autenticidad del certificado enviado por **A**.

- ***Grafico 5*:**



1. **A**, solicita la emisión de un certificado de firma electrónica al Tercero Vinculado (**3V**).
2. **3V** previa a la verificación de la identidad del solicitante, pedirá a la Entidad de Certificación (**EC**) que expida el correspondiente certificado. **EC** recibe la solicitud con la identidad verificada del titular, proporcionándole el certificado a **3V**.
3. **3V** procede con la entrega del certificado a **A**, el cual fue emitido por la entidad certificadora.
4. **A** encripta su mensajes de datos y lo envía a **B** conjuntamente con el certificado que recibió de **3V**. **B** descifrará la firma electrónica con la clave pública de **A** obteniendo el mensaje original.
5. De manera facultativa, **B** podrá acceder al repositorio de la **EC**, a fin de verificar la validez de certificado.

2.2.1 Clasificación de Procesos de Emisión

Dentro del proceso de emisión de certificados de firma electrónica, ciertas legislaciones y doctrinas internacionales han decidido darle una clasificación especial para cada caso, deviniendo en tres tipos:

- *Certificación Simple*; sucede cuando una Entidad de Certificación única, avala la tecnología y prácticas en todas sus partes, emitiendo también los certificados y pares de claves criptográficas, donde además llevaría un registro de las transacciones que realice.
- *Certificación Cruzada*; generalmente se produce en el reconocimiento de certificados de firma electrónica extranjeros, ya que la clave pública es certificada por varias Entidades de Certificación. "En tales casos es necesario que entidades de certificación sustancialmente equivalentes (o entidades certificadores dispuestas a asumir ciertos riesgos con respecto a los certificados emitidos por otras entidades certificadoras) reconozcan mutuamente los servicios prestados, de forma que los respectivos usuarios puedan comunicarse entre ellos de manera mas eficaz y con mayor confianza en la fiabilidad de los certificados que emitan."[35]
- *Certificación Jerárquica*; se genera en razón del escalafón de entidades, es decir, cuando uno o varios Terceros Vinculados, situadas bajo una Entidad de Certificación, certifican que la clave pública de un usuario corresponde en realidad a la clave privada del mismo usuario.

2.3 Proceso de Acreditación

Dentro del ámbito mundial, por regla general, las entidades de certificación y sus subsidiarias están bajo la regulación y control de entidades gubernamentales, donde cada Estado deberá establecer sus propios lineamientos que se deban cumplir para la acreditación de las entidades. "Los sistemas gubernamentales o privados de certificación se completan con la intervención de una autoridad de control, que depende de algún órgano de gobierno y que vigila el funcionamiento del sistema, pudiendo establecer la necesidad de una autorización previa para que funcionen las autoridades de certificación y estableciendo un registro obligatorio o voluntario de tales entidades."[36]

[35] DEVOTO Mauricio; *Comercio electrónico y firma digital*; p. 174
[36] HOCSMAN Heriberto Simón; *Negocios en Internet*; p. 398

En el caso ecuatoriano existen dos sujetos de derecho público destinados al control y regulación de las entidades de certificación. En primera instancia se encuentra el *Consejo Nacional de Telecomunicaciones* (**CONATEL**), organismo encargado de regulación, autorización y registro de las entidades de certificación; dentro de sus funciones substanciales se encuentra el cancelar o suspender la autorización de funcionamiento a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones, y también el revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emite con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones.

Por otro lado, la *Superintendencia de Telecomunicaciones* **(SUPTEL),** es el organismo delegado al control y fiscalización de las entidades de certificación, contando además con la facultad de imponer sanciones administrativas por incumplimiento de sus obligaciones.

Para poder operar legalmente dentro del Ecuador, los peticionarios deberán entregar a la *Secretaría Nacional de Telecomunicaciones* (SENATEL) los siguientes documentos: a) solicitud dirigida a la SENATEL; b) copia de cédula de ciudadanía y papeleta de votación del representante legal; c) copia certificada e inscrita en el Registro mercantil de la escritura de constitución de la compañía o empresa y del nombramiento del representante legal; d) original del Certificado de Cumplimiento de Obligaciones de la superintendencia a la que corresponda; e) descripción técnica de la infraestructura a ser utilizada y sus recursos; f) descripción de cada servicio propuesto; g) documentos de soporte que confirmen la disposición de mecanismos de seguridad electrónica; h) ubicación geográfica inicial y ubicación de cada *nodo*[37], incluyendo un diagrama técnico de estos, e; i) documentación que demuestre solvencia económica.

Habiendo solicitado lo anterior, el peticionario requerirá de la *Acreditación*, esto se efectuará por medio de un acto administrativo, en donde la SENATEL deberá en el término de tres días, publicar en su página Web, un extracto de la solicitud. Conjuntamente, contará de 15 días para remitir un informe técnico, legal y económico del solicitante al CONATEL, el cual a su vez, dentro de 15 días término, resolverá sobre el otorgamiento. Dicha resolución será entregada a la SENATEL a fin de que proceda con la

[37] Un nodo es un punto de intersección o unión de varios elementos que confluyen en el mismo lugar. Por ejemplo, en una red de ordenadores cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también un nodo.

inscripción en el *Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditados y Terceros Vinculados* (RPNE), el cual se encuentra a su cargo, previo a la consignación del pago de un valor monetario, el cual es determinado por la misma autoridad autorizante, por concepto de derechos de permiso; caso contrario, si el solicitante no cumpliere con el desembolso en el término de 15 días, el acto administrativo quedará sin efecto procediendo al archivo del trámite.

Según Resolución 480-20/08 emitida por el CONATEL con fecha ocho de octubre de 2008, se estipuló que el valor por acreditación y registro necesarios para el perfeccionamiento del reconocimiento legal será de diez mil dólares de Estados Unidos de América, tanto para las entidades de certificación y terceros vinculados e igualmente se consignará el valor de seis mil dólares americanos para la prestación de servicios de certificación de información y servicios relacionados.

Conjuntamente se depositará una garantía monetaria de cuatrocientos mil dólares (*este valor fue modificado en la Reforma al Reglamento General, siendo anteriormente de un millón de dólares según la Res. 324-17/06*), por concepto de responsabilidad, con el fin de asegurar a los usuarios el pago por posibles daños y perjuicios ocasionados por incumplimiento de obligaciones por parte de la Entidad de Certificación. Este valor variará anualmente según los informes de fiscalización emitidos por la Superintendencia de Telecomunicaciones y en función de un valor base de garantía por certificado, determinado por el CONATEL.

Finalmente se pagará por gastos de administración, el valor de tres mil dólares al CONATEL y SENATEL, y tres mil dólares más a la Superintendencia de Telecomunicaciones por gastos de control.

Tabulando dichos valores, se los entiende de la siguiente manera:

Emisión de Acreditación y Registro	USD 10.000
Prestación de Servicios: *emisión de firmas electrónicas, sellado de tiempo, conservación de mensajes de datos y otros servicios relacionados*	USD 6.000
CONATEL y SENATEL	USD 3.000
SUPTEL	USD 3.000
TOTAL	**USD 22.000**

Por lo tanto, teniendo inexcusablemente que realizar una inversión considerable para cumplir con las políticas de solvencia técnica (lo cual considero extremadamente

necesario), se debe disponer de un capital medianamente alto para gastos administrativos, dando como resultado, en el caso de estar interesados en constituir una Entidad de Certificación Acreditada en el Ecuador, la cual cuente con todos los servicios requeridos en el mercado (emisión de firmas electrónicas y certificados, sellado de tiempo y conservación de mensajes de datos), ésta requerirá un capital de cuatrocientos veinte y dos mil dólares americanos.

En lo referente a la garantía de responsabilidad, esta podrá consignarse ya sea mediante una póliza de seguro de responsabilidad (contemplado en el Art. 43 de la Ley General de Seguros) u otorgando una garantía bancaria, conforme a la facultad concedida a las instituciones financieras en el Art. 51 literal c) de la Ley General de Instituciones del Sistema Financiero.

De darse el incumplimiento de obligaciones por parte de la Entidad de Certificación ocasionando daños y perjuicios a un usuario, éste deberá presentar en el término de 15 días, contados desde la ejecución del perjuicio, una solicitud motivada ante la SENATEL, la cual deberá poner en conocimiento del reclamo a la Entidad de Certificación, a fin de que en el término de cinco días reconozca la infracción o presente descargos. Cumplido el plazo, la SENATEL resolverá el reclamo. De ser favorable la resolución para el usuario, deberá disponer a la compañía aseguradora o institución financiera, el desembolso parcial de la garantía.

Ahora bien, el Título Habilitante representa la acreditación y permiso para la prestación de servicios de certificación y servicios relacionados. Este permiso comprende los derechos de instalación, modificación, ampliación y operación de la infraestructura requerida para brindar dichos servicios, cuya vigencia será de diez años, los cuales podrán ser prorrogados por igual tiempo, previa solicitud escrita del interesado, con tres meses de anticipación al vencimiento del plazo original.

Habiendo la SENATEL otorgado la Acreditación al peticionario, éste dispondrá de un plazo de seis meses para iniciar sus operaciones, y será obligación de la Superintendencia de Telecomunicaciones el verificar que se cumpla con este requisito, caso contrario, deberá informar a la SENATEL dicho incumplimiento a fin de que proceda con la extinción del permiso, salvo el caso de que el permisionario haya requerido ampliación en el plazo mediante solicitud motivada ante la SENATEL, la cual contará de 15 días perentorios a fin de que conceda o niegue el requerimiento.

La ampliación no podrá ser por un plazo mayor a 90 días y se otorgará por una sola vez; cabe mencionar que como toda petitoria ante autoridad pública, esta se rige por las normas

generales del silencio administrativo, fallándose favorablemente para el solicitante en caso de no haber respuesta en el termino de 15 días.

Una vez cumplidas estas diligencias, el requirente se encuentra facultando legalmente para operar como Entidad de Certificación *Acreditada*, siendo el único beneficiario durante todo el tiempo de ejercicio, ya que por prohibición legal, no podrá ceder ni transferir a un tercero los derechos adquiridos.

2.3.1 Acreditación de un Tercero Vinculado

De forma similar, el trámite de acreditación para un Tercero Vinculado se lo realizará mediante una solicitud ante la SENATEL, en la cual deberá adjuntar los mismos documentos previamente enumerados para las Entidades de Certificación, a excepción de los literales g), h) e i). Adicionalmente, constituye requisito esencial, la presentación de documentos que legitimen la relación contractual con la Entidad de Certificación de Información y Servicios Relacionados Acreditada, donde constará claramente las responsabilidades legales de cada uno de los contratantes respecto de los usuarios y autoridades.

Contando desde la fecha de presentación de la solicitud, la SENATEL dentro de 15 días adjudicará al interesado el certificado de registro. La constancia del mencionado registro gravitará en una razón o marginación efectuada por la Secretaria Nacional de Telecomunicaciones, dentro del *Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditados y Terceros Vinculados*.

2.3.1 Acreditación de Entidades Públicas

Constituyéndose un avance para el Ecuador, en lo concerniente a la práctica de la tecnología informática - como ya se hizo referencia – en sesión 20ª de 2008 del Consejo Nacional de Telecomunicaciones, se autorizó al Banco Central del Ecuador como la primera Entidad de Certificación Acreditada de derecho público, cumpliendo a cabalidad el acto administrativo correspondiente, el cual se efectuó con celeridad y eficiencia, donde las autoridades envueltas en la acreditación supieron respetar los plazos legales establecidos.

Las instituciones públicas que pueden acceder a esta calidad serán los organismos y dependencias de las funciones Legislativa, Ejecutiva y Judicial, así como todas aquellas entidades y organismos creados y contemplados por la Constitución Política o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para el desarrollo de actividades económicas asumidas por el Estado.

En lo pertinente al proceso de acreditación para entes estatales deviene a ser el mismo que el de las Entidades de Certificación privadas, otorgando dentro del noveno artículo innumerado agregado por el artículo cuarto de la Reforma al Reglamento General a la Ley de Comercio Electrónico, la facultad excluyente para las certificadoras estatales de emitir certificados de firma electrónica para las instituciones públicas.

2.4 Contrato entre Entidad y Usuario

El contrato que las entidades de certificación o registro suscriban con sus usuarios es de vital importancia por cuanto a través de este instrumento se formaliza la atribución de autoria de todos los mensajes de datos que el consumidor remita a terceros, negándole además cualquier posibilidad de repudio respecto de la información enviada.

De esta manera, todo texto firmado digitalmente alcanzará el nivel jurídico de firma manuscrita, superando el factor de rechazo que tiene la firma autógrafa, por ser un método de presunción de autoría, obligándose al cumplimiento de todo aquello estipulado en el documento.

"Una firma (*electrónica*) podía constituir un testimonio de la intención de una parte de considerarse vinculada por el contenido de un contrato firmado, de la intención de una persona de respaldar la autoría de un texto (manifestando así su conciencia de que del acto de la firma podrían derivarse consecuencias jurídicas), de la intención de una persona de asociarse al contenido de un documento escrito por otra persona, y del hecho de que una persona estuviera en un lugar determinado en un momento determinado."[38]

Dentro del presente contrato, cada interviniente posee dos obligaciones primordiales que deberán cumplir:

- *Entidad de Certificación*; 1. Deberá certificar la identidad de su consumidor; 2. Emitir el correspondiente certificado de firma electrónica, el cual deberá contar con acceso informático.

[38] CNUDMI; *Ley Modelo…*; p. 23

- *Usuario*; 1. Mantener reserva respecto de su clave privada; 2. Notificar de manera oportuna, si existe el hecho presunto o fehaciente de que un tercero tenga conocimiento de dicha clave, a fin de que la Entidad proceda a suspender o revocar los certificados de firma electrónica.

A más de lo estipulado, constituye requisito esencial de la Entidad de Certificación, el determinar el plazo de vigencia de los certificados que se emitan.

Dentro de la legislación ecuatoriana se articula la necesidad de la aprobación por parte del CONATEL respecto de estos contratos, conservando además la facultad de consentir cualquier tipo de modificación ulterior que se realice; debiendo estos contratos ser emitidos dentro del territorio ecuatoriano, en idioma castellano y estar sometidos a la jurisdicción y a las leyes ecuatorianas.

3. INFRAESTRUCTURA DE CLAVE PÚBLICA

Como ya se mencionó la infraestructura de clave pública o *Public Key Infrastructure (PKI)* la constituyen los programas y equipos, sistemas de información, redes electrónicas de información, políticas y procedimientos cuya finalidad es soportar la operación de los servicios de certificación de información y servicios relacionados, "ello tienen como objetivo brindar la mayor seguridad posible y generar la consecuente confiabilidad para los usuarios."[39]

Dicha infraestructura es de existencia imperante dentro del funcionamiento pleno de la firma electrónica ya que abarca, a parte de los sistemas y políticas de operación, a los sujetos jerárquicamente superiores e inferiores de las entidades de certificación.

De esta manera, la estructura de clave pública comprende determinadas garantías y servicios a sus involucrados:

- *Servicios*; 1) emisión de firmas electrónicas y sus certificados; 2) Certificación electrónica; 3) Conservación de Mensajes de datos; 4) Comprobación de la identidad de los usuarios; 5) publicación de repositorio, entre otros.
- *Garantías*; 1) No alteración de las claves públicas y vinculación inequívoca con el usuario; 2) sistemas que garanticen la confiabilidad en la transferencia de mensaje de datos; 3) técnicas fiables de encriptación.

[39] SARRA Andrea; *Comercio electrónico y derecho*; p. 392

3.1 Jerarquía Estructural

En base a lo mencionado, nace un escalafón dentro de la infraestructura de clave pública, el cual consta según las funciones e importancia de los miembros que abarcan el universo práctico de la firma electrónica.

- *Entidad de Fiscalización y Control*; Esta entidad se encarga del control y observancia de las políticas generales de funcionamiento, debiendo además realizar auditorías técnicas de las entidades de certificación y emitir informes motivados. En el Ecuador esta función está a cargo de la Superintendencia de Telecomunicaciones (SUPTEL).
- *Entidad de Inscripción y Acreditación*; Ésta estará delegada a la aprobación, suspensión y cancelación de las autorizaciones de funcionamiento de las Entidades de Certificación, de la Acreditación de funcionamiento y además estará obligada de llevar un registro de todas las Entidades de Certificación.

  En algunas legislaciones, como es el caso de Ecuador o España, se dividen las funciones de inscripción y acreditación en entidades distintas. La inscripción abarca la autorización, registro y regulación de las entidades, lo cual está a cargo del CONATEL. Mientras que la acreditación, que se realiza a través de la Acreditación legal, la cumple la SENATEL.

  Esta distinción es facultativa ya que el cumplimiento de estas obligaciones las puede realizar una sola autoridad.
- *Entidad de Certificación*; Es el tercero de confianza constituido por una persona jurídica, pública o privada, cuya función principal es la de emitir certificados de firma electrónica permitiendo de esta manera, la vinculación del suscriptor con la firma y determinando la identidad del mismo.

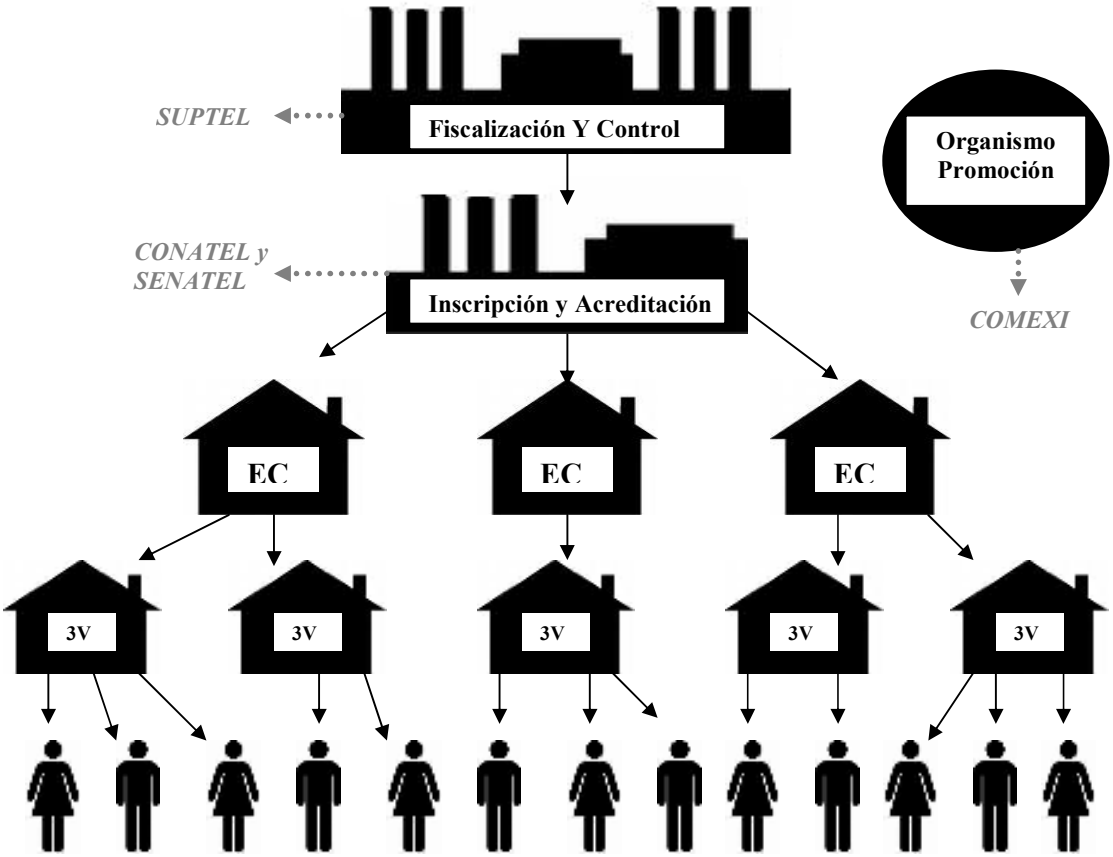
  Dentro de algunos países, por razones de orden público, estas entidades únicamente podrán ser sujetos de derecho público.
- *Tercero Vinculado*; Como ya revisamos, estas son jerárquicamente inferiores que las de certificación y cumplen con funciones específicas como la recepción de datos, verificación y entrega de los certificados que son emitidos por la Entidad de Certificación.
- *Usuarios*; Son personas naturales o jurídicas, nacionales o extranjeras, titulares de un par de claves (pública y privada), cuya actividad radica en solicitar certificados de firma electrónica y custodia de su clave privada.
- *Organismo de Promoción*; Esta entidad se encuentra contemplada dentro del artículo 36 de la Ley de Comercio Electrónico, cuya finalidad consiste en promover y difundir

los servicios electrónicos, el comercio electrónico y el uso de las firmas electrónicas respecto a la ejecución de inversiones y comercio electrónico. La presente actividad estará a cargo del *Consejo de Comercio Electrónico e Inversiones* (COMEXI).

En esencia, el COMEXI está conformado por representantes de los sectores público y privado, donde su función radica en establecer un nexo entre esos sectores, buscando la apertura de mercados mediante el comercio exterior y dedicándose también a alentar la modernización del Estado.

A la presente estructura jerárquica la podemos entender gráficamente de la siguiente manera:

- Gráfico 6:



CAPÍTULO IV
IMPLICACIONES JURÍDICAS DE LOS MENSAJES DE DATOS

Finalmente hemos dilucidado el desarrollo técnico, jurídico y comercial que se halla enmarcado en la esfera de la firma electrónica, la cual nos pone a disposición un medio transaccional seguro respecto al envío y recepción de mensajes de datos, construyendo así una sociedad que avanza de manera paralela con las nuevas tecnologías, imponiéndose a los documentos escritos, ya que los instrumentos electrónicos son transformados en actos jurídicos reconocidos, determinando el cumplimiento veraz por parte de los actuarios en referencia a sus obligaciones contenidas. ¿Pero, exactamente en qué basa su juridicidad y cuales son sus alcances? ¿A qué determinamos como mensaje de datos? ¿Qué actividades públicas y privadas se pueden realizar por este medio? ¿Cuál es el marco jurídico de mis relaciones internacionales? Estas son algunas de las interrogantes respecto a la actividad práctica que pretendo esclarecer en el presente Capítulo.

1. EL DOCUMENTO

Como paso previo para adentrarnos al entorno del desenvolvimiento práctico del mensaje de datos, es necesario aclarar su concepción y raíces con una pequeña reseña de su nacimiento y terminología.

El mensaje de datos se origina en los documentos, los cuales existen desde la evolución histórica de la escritura. Se puede entender al documento, en un sentido amplio tomando en consideración el avance progresivo de la tecnología, como la declaración de un hecho o información de cualquier tipo, la cual es plasmada o ilustrada en cualquier medio fehaciente. Por otra parte Chiovenda lo ha definido como "toda representación material destinada e idónea para reproducir una cierta manifestación del pensamiento"[40].

[40] CHIOVENDA, Giuseppe; *Instituciones de Derecho Procesal Civil*; Revista de Derecho Privado, Madrid, 1940, p. 265.

En razón de la costumbre, se ha considerado al documento como sinónimo de un instrumento escrito, físicamente palpable, noción que con el tiempo ha ido variando con la práctica informática y jurídica, dando como resultado una clasificación, donde los dos primeros se perpetran en razón del soporte, los dos siguientes por concepto de vinculación de autoría y los últimos por su creación:

- *Documento físico*; consiste en la manifestación expresa, cuya exteriorización radica en medios materiales, es decir, de percepción táctil. Ejemplo de esto es una carta escrita sobre papel.
- *Documento electrónico*; conocido en nuestra legislación como mensaje de datos, es aquel cuya expresión versa en medios telemáticos, cuyo asentamiento reside en bits, los cuales son demostrables pero no ciertos en materia corporal. Esto puede ejemplificarse con la elaboración de un correo electrónico.
- *Documento firmado*; es aquel instrumento donde se hace constar una rúbrica que vincula al autor con el texto; Esta firma podrá ser ológrafa o electrónica, siendo ambas de reconocimiento legal. Este hecho se demuestra con un contrato, donde las partes expresan su voluntad de obligarse.
- *Documento no firmado*; texto en el cual existe manifestación de voluntad por parte de su autor, pero el nexo de sujeto-instrumento no es demostrable de forma irrefutable. Podemos demostrar esto con el supuesto de un mensaje anónimo, en donde la vinculación de autoría se la hará por medios externos como el peritaje grafológico o técnico.
- *Documento original*; Es aquel primerizo, primitivo o de carácter primario. Es considerado como el instrumento inicial o base.
- *Documento duplicado*; Consiste en la fiel copia de un original, la cual puede ser efectuada por parte del autor o de un tercero, constituyendo esto último en una posible falsificación.

Finalmente, los documentos contienen valores jurídicos diferenciables, catalogándose de la siguiente forma:

- *Documentos Constitutivos*; son aquellos en donde conjuntamente con su nacimiento aparece un derecho para posteriormente deslindarse de él. Es el caso de los testamentos.
- *Documentos Constitutivos-Dispositivos*; donde el nacimiento del documento y el derecho son simultáneos y se vinculan mutuamente, siendo necesaria la presencia del documento para el ejercicio del derecho. Por ejemplo, las letras de cambio.

- *Documentos probatorios*; los cuales involucran la declaración de un derecho o vínculo jurídico, con carácter probatorio. Esto puede suceder con las cartas poderes que son presentadas ante la Junta General de una compañía para exigir la participación dentro de ella.

Cabe mencionar que, indistintamente estos preceptos son aplicables tanto para los documentos físicos como los electrónicos.

2. MENSAJE DE DATOS

Los mensajes de datos constituyen un entorno amplio en el cual se engloba toda clase de información contenida en un soporte el electrónico, es por esto que nuestra ley de Comercio Electrónico en la disposición novena, destinada como glosario de términos, ha definido los mensajes de datos como "toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que ésta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, servicios web, telegrama, télex, fax e intercambio electrónico de datos."

En base a lo mencionado podemos establecer que los mensajes de datos son toda declaración almacenada por medios digitales con efectos jurídicos, la cual se efectúa por una serie de combinaciones numéricas binarias, cuya exteriorización radica en la utilización de un hardware y software.

Respecto al tema, Sarra conceptúa por cuerda separada la definición de documento electrónico diciendo que "se denomina 'documento' a la entidad jurídica que constituye un 'instrumento' (…) *mientras* el término 'electrónico' hace referencia al dispositivo en el que está almacenado el instrumento."[41]

3. ÁMBITO JURÍDICO

En la ejecución práctica de los mensajes de datos por medio de firma electrónica, existe normativa la cual regula su desenvolvimiento; es por esto que a continuación me permito

[41] SARRA Andrea; *Comercio electrónico y derecho*; p. 346

describir los alcances y limitaciones concedidos a la documentación electrónica dentro de la legislación.

3.1 Reconocimiento Legal

Dentro de la Ley Modelo de Comercio Electrónico de la CNUDMI estableció el principio de equivalencia funcional, el cual otorga una aplicación idéntica al documento físico como al electrónico ya que éste último brinda mayores garantías que el primero. "Dado que una firma manuscrita no garantiza la integridad del documento al que se adjunta ni garantiza que puedan detectarse eventuales cambios introducidos en el documento."[42]

Este hecho queda respaldado con el artículo cinco de la misma ley, que dice "No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos."[43]

La mención viene a ser bastante lógica ya que ambos contienen los mismos elementos de existencia:

- *Soporte*; es la base en donde radica la manifestación, pudiendo ser física o magnética.
- *Exteriorización*; esto será a través de un lenguaje entendible, la diferencia consta en el medio que se utiliza para trasladar la información al soporte, por una parte podrá ser simplemente un lápiz o pluma, mientras que en el campo informático se lo haría por códigos o dígitos.
- *Manifestación*; es el mensaje que contiene la manifestación del pensamiento o voluntad de su autor.

Esta información fue tomada como fundamento para el reconocimiento legal por parte de la legislación ecuatoriana, ya que la ley de Comercio Electrónico tipificó lo propio diciendo que "los mensajes de datos tendrán igual valor jurídico que los documentos escritos." De esta manera quedan eliminados los problemas en la actividad comercial, dejando claro que cualquier obligación adquirida por medios electrónicos acarreará efectos jurídicos.

[42] http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf ; p. 62
[43] http://www.zur2.com/objetivos/leyextran/cnudmi.htm

3.2 Incorporación por Remisión

Dentro de nuestra normativa, tanto en la Ley de Comercio Electrónico (Art. 3) como en su Reglamento General (Art. 1), instituye legalidad a la información que se halle incorporada por remisión, en otras palabras, se valida toda documentación anexa que hubiere sido conjuntamente enviada con el mensaje de datos, cuyo acceso se lo realice por medio de un enlace contenido en el mismo.

En cuanto a las relaciones comerciales que involucre a proveedores y consumidores, se deberá establecer de manera expresa la remisión, debiendo ésta contar con un acceso sencillo y aceptable. Esto se corrobora con la obligación que tiene el proveedor de brindar a sus consumidores, información adecuada, veraz, clara, oportuna y completa sobre los bienes y servicios que ofrece, incluyendo los riesgos que pudieren prestar. Debiendo regir sus transacciones comerciales según lo estipulado dentro de la Ley Orgánica de Defensa del Consumidor.

Tanto en las relaciones entre particulares y de consumidores, en caso de que la información contenida en los anexos sufra variantes, será obligación del emisor, notificar oportunamente de los cambios al receptor del mensaje, por los mismos medios electrónicos o por escrito, debiendo en su comunicado resaltar las modificaciones que se han suscitado, para que el destinatario de su aceptación de manera expresa.

Posteriormente, los mensajes de datos y sus anexos deberán ser asequibles de forma indefinida para su posterior consulta, contando con los mecanismos necesarios para tal efecto.

3.3 Propiedad Intelectual

Como es de noción colectiva, la propiedad intelectual consiste en reconocer a determinado sujeto la propiedad de obras provenientes de su intelecto, las cuales se hacen merecedoras de protección respecto a terceros. En motivación de lo dicho, la legislación ha velado por las invenciones científicas y tecnológicas, las producciones literarias o artísticas que pudieren producirse o difundirse por métodos electrónicos, determinando así que "los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual"[44]

[44] Ley de Comercio Electrónico, firmas electrónicas y mensaje de datos; Art. 4

Este concepto subsiste en concordancia con la normativa interna y externa existente. Respecto al fuero interno de reglamentación estatal, el Ecuador ha reconocido a las invenciones de carácter intelectual como derecho fundamental de los ciudadanos, donde el estado se arroga la obligación de protegerlos, delegando su cumplimiento al Instituto Ecuatoriano de Propiedad Intelectual. Esta entidad ha expedido la Ley de Propiedad Intelectual, cuya vigencia data de 1998, la cual reconoce y garantiza los derechos de los autores y los derechos de los demás titulares sobre sus obras.[45]

La propiedad intelectual es considerada de vital importancia para el desarrollo tecnológico y económico de las naciones, permitiendo una explotación excluyente del autor referente a sus obras. Gracias al reconocimiento internacional que existe, se han desarrollado verdaderos imperios económicos los cuales han inyectado el capital necesario para el crecimiento de los Estados, tal es el caso de *The Coca-Cola Company*, la cual existe desde 1885, que como resultado de la protección intelectual dada a su fórmula, ha alcanzado su comercialización a más de 200 países en todo el mundo; solo bastó un año de reserva en el proceso de elaboración para que a su creador le sean ofrecidos 2.300 millones de dólares a fin de que el producto sea colocado en todo el territorio norteamericano.

A este suceso se lo puede considerar como el factor que catapultó la normativa de protección mundial, desde ese entonces se ha tipificado normas y tratados de aplicación internacional, es así que convenios como el de Berna para la Protección de Obras Literarias y Artísticas realizado en el año de 1886, tomando como base la iniciativa dada en Francia en 1883 con el Convenio de París para la Protección Industrial.

A pesar de todos estos esfuerzos, en la actualidad se han registrado infracciones considerables que han sido ejecutadas por medios informáticos; tal es el caso del programa *Napster*, que en 1999 sus titulares fueron enjuiciados por varias disqueras, ya que prestaban el servicio de distribución y descarga de música por medio del Internet, evadiendo el pago de derechos de autor[46]. Empero de ello, aún continúan apareciendo programas con las mismas prestaciones.

[45] Art. 4; *Ley de Propiedad Intelectual*; RO/ 320 de 19 de Mayo de 1998.
[46] http://news.bbc.co.uk/2/hi/business/1000463.stm

3.4 Confidencialidad y Protección de Datos

Tanto la confidencialidad,como a la protección de información privada, se las puede considerar como principios fundamentales, no solo en las relaciones de carácter electrónico, sino en la vida diaria de las personas.

Esta afirmación no queda únicamente sustentada en el recuerdo histórico de la actividad social, por el contrario, a lo largo de la vida constitucional del Ecuador, así como de los países que se encuentran territorialmente envueltos en nuestra región, ha sido tomado de manera amplia y vasta las consideraciones referentes a los derechos de los ciudadanos, convirtiendo a la parte dogmática de nuestra Carta Política, en el sustento y anhelo de sus gobernados.

Es así que, siguiendo este lineamiento, nuestra Ley Suprema vigente desde octubre de 2008, consta con más de noventa artículos (superior al veinte por ciento del texto constitucional) destinados a los principios, derechos y garantías constitucionales de las personas, sin tomar en cuenta a los setenta y cinco artículos referentes al buen vivir o *Sumak Kausay* (por su definición en Quechua), título cuyo articulado versa sobre recaudados a la población en temas transcendentales como educación, salud, seguridad, cultura, entre otras. En este punto solo queda en manos de nuestros gobernantes el cumplir y respetar estas disposiciones, para que no se violente el ansia y decoro del pueblo que busca una conversión hacia la realidad de estos preceptos, ya que, como dice el doctor Hernan Salgado, "para las mayorías populares los derechos tienen sentido a partir del momento en que se transforman en exigencias satisfechas"[47].

De esta manera, dentro del inmenso conjunto de derechos, se ha incluido acertadamente las disposiciones vinculantes a este caso; solo por enumerar unas pocas, dentro del artículo 66 numeral 19 y 21, nuestra Constitución reconoce a sus pobladores

> "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" y "El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación."

[47] SALGADO Pesantes, Hernán; *Lecciones de derecho constitucional*; 1996; tercera edición; Ed. Ediciones Legales; Quito-Ecuador; p. 152

De manera conjunta y delimitada en el ámbito electrónico, la Ley de Comercio Electrónico (Art. 5) sanciona la violación de estos derechos, determinando de manera especial a la intrusión electrónica, transferencia ilegal de mensajes de datos y a la violación de secreto profesional que haya sido transferida por medios informáticos. En igual forma en consideración a la protección de datos, el mismo cuerpo legal se tipifica que para cualquier forma de utilización de bases de datos obtenidas por medio de transmisión electrónica, requerirá el consentimiento expreso de su autor, estableciendo como salvedad del consentimiento al hecho de recopilación de datos de fuentes accesibles al público cuando su fin sea ejercer las funciones de la administración pública.

Las sanciones a las que se refiere nuestra Ley de Comercio Electrónico se encuentran tipificadas dentro del Código Penal, en el cual se halla la violación a los delitos contra la información protegida (Art. 202.1), obtención y utilización no autorizada de información (Art. 202.2), destrucción maliciosa de documentos (Art. 262), falsificación electrónica (Art. 353.1), daños informáticos (Art. 415.1), apropiación ilícita de bienes (Art. 553.1) y como contravención de tercera clase, la violación del derecho a la intimidad según los parámetros de la Ley 67 (Art. 606 Inc. 20).

3.5 Desmaterialización de Datos

Algo que hemos repetido infinidad de veces y consecuentemente constituye una realidad, es que la actividad comercial avanza de manera desmesurada, por lo que los accionarios comerciales han utilizado como herramienta fundamental al Internet, garantizando legalmente sus negociaciones y acuerdos mediante la firma electrónica, poniendo en práctica al *e-commerce*[48].

Pero se debe tomar en cuenta que toda la documentación encerrada en una transacción comercial no radica exclusivamente en los documentos elaborados por los comerciantes, existen instrumentos necesarios que son expedidos por terceros. Por ejemplo, al constituir una relación comercial de exportación, puede darse el supuesto de que el exportador debe hacer llegar la documentación de desaduanización al importador a fin de que retire la mercancía enviada; en este caso se crea un factor que retrasaría e incrementaría el costo

[48] El *e-commerce* consiste en la compra, venta y marketing de mercancías y servicios a través de medios informáticos. A esta actividad no se la debe confundir con el *e-business*, la cual a más de incluir los elementos del e-commerce involucra procesos internos de la compañía como administración, desarrollo de estrategias, relaciones con proveedores, distribuidores y empresas relacionadas, entre otras.

operacional, por cuanto el exportador necesitará del correo tradicional para enviar el título en cuestión. Es aquí donde se aplica a la desmaterialización de documentos.

La desmaterialización consiste en una copia electrónica idéntica del documento físico original, siendo esta copia portadora de los mismos efectos que aquellas certificadas por la autoridad competente.

Dentro del Reglamento General a la Ley de Comercio Electrónico (Art. 5) se delimita el proceso de aplicación para la desmaterialización de documentos. Como obligación primordial se menciona la necesidad del acuerdo expreso de los involucrados, respecto a la aceptación de desmaterializar los documentos. Esta aceptación podrá constar en un documento físico o electrónico (con las debidas firmas digitales para el segundo caso).

Volviendo a nuestro ejemplo anterior, los legisladores han prevenido los casos que la ley o las partes exijan solemnidades, estableciendo como fedatario al Notario Público, debiendo este último certificar de manera electrónica, que la copia desmaterializada contiene características idénticas que el original. Fundando de completa validez jurídica a la copia del título de desaduanización que recibirá el importador, pudiendo completar exitosamente con la negociación que usamos como ejemplo previamente.

Existen características especiales respecto a los documentos desmaterializados:

- *Marginación*; el documento desmaterializado deberá constar de una razón o marginación que determine el hecho de ser la desmaterialización del instrumento original.
- *No duplicación de obligaciones*; en caso de que los documentos desmaterializados contengan obligaciones para las partes o para terceros, se entenderá como la manifestación de un mismo acuerdo, negando la multiplicación de responsabilidades, siendo estas una sola.
- *Multiplicidad de documentos*; de existir diversidad de instrumentos originales y desmaterializados, salvo prueba en contrario, se concebirán como fieles copias de un solo documento.

3.6 Calidad Probatoria

La acción probatoria en términos generales consiste en la justificación respecto a la certeza de determinados hechos afirmativos para así establecerlos como reales.

Esta actividad la empleamos en todas las etapas de nuestras vidas, desde que somos pequeños buscamos los medios para probar que no rompimos un plato o un florero cuando nuestros padres nos imputan ese descuido, de la misma manera conforme vamos creciendo nos son planteados ciertos parámetros para demostrar nuestras afirmaciones, es así como en la vida estudiantil tenemos procedimientos preestablecidos para probar la veracidad de nuestros cálculos matemáticos, y finalmente cuando llegamos a la etapa adulta, los legisladores han plasmado en códigos los métodos para manifestar la autenticidad de nuestros actos procesales que se encuentran contrapuestos con afirmaciones de terceros, para que un Juez sea quien establezca la existencia o inexistencia de lo expuesto.

La comprobación de nuestros actos constituyen una necesidad en la vida humana, ya que, como menciona Serra Domínguez "… los hombres, en cuanto fiables y mendaces, requieren inexcusablemente comprobar la exactitud de las diversas afirmaciones que otros hombres les proponen."[49], esto queda demostrado en concordancia con la teología moral del hombre, donde éste hará uso de cualquier vía con el fin ulterior de alcanzar su cometido.

Es por estos motivos que el comercio electrónico no ha sido la excepción, por cuanto en las comunicaciones a través de mensajes de datos con firmas electrónicas, se encuentran inmersos intereses y obligaciones, que de no ser cumplidos, se requerirá comprobar la veracidad de lo estipulado, para así exigir su cumplimiento y sanear los perjuicios causados. En razón de esto, la Ley de Comercio Electrónico (Ley 67) en sus artículos 52 y 54, ha decretado que las firmas electrónicas, mensajes de datos y certificados de firmas electrónicas nacionales o extranjeros, que hayan sido emitidos conforme a la Ley, tendrán carácter probatorio, debiendo además respetar las disposiciones establecidas en el Código de Procedimiento Civil (*CPC*). En el mencionado cuerpo legal se ratifica esta aseveración disponiendo en el Art. 121 que *los documentos obtenidos por medios técnicos, electrónicos, informáticos, telemáticos o de nueva tecnología* también son admitidos como medios de prueba, con la misma valoración legal que los tradicionales como son las declaraciones testimoniales, inspecciones judiciales, informes periciales, etc.

Ahora bien, por ser esta una situación ajena a los escenarios comunes, existen reglas específicas para la práctica de la prueba:

- *Mensaje de datos en juicio*; cuando se utilice un mensaje de datos como medio de prueba dentro de un proceso judicial, el interesado deberá incluir el soporte electrónico

[49] SERRA DOMÍNGUEZ Manuel; *Estudios de Derecho Procesal*; Ed. ARIEL; Barcelona-España 1969; p. 355

y físico (*papel*) del mensaje. Y de ser requerido, le corresponderá facilitarle al Juez o Tribunal todos los elementos necesarios para su estudio y verificación.

- *Impugnación de firma electrónica o de certificado*; dada la impugnación por cualquiera de las partes respecto a una firma electrónica o su certificado, será obligación del interesado requerirle al Juez o Tribunal que solicite a la Entidad de Certificación la remisión de información certificada competente a la deferencia.
- *Datos desmaterializados*; el facsímile o copia de un documento físico enviado como mensaje de datos, también constituyen medio de prueba, siempre y cuando se hayan respetado las normas de desmaterialización de datos.
- *Invalidez del mensaje de datos*; en el supuesto de que una de las partes niegue la validez de un mensaje de datos, esta estará en la obligación de demostrar los vicios que le invalidan o las falencias dentro del proceso de seguridad que lo hicieron vulnerable. En este caso cabe la comprobación técnica para la verificación de los hechos.

Como hemos visto, generalmente las normas que han sabido establecer nuestros legisladores acerca del comercio electrónico, van en relación con los tratados internacionales que el Ecuador se encuentra inmerso; dentro del artículo nueve, numeral dos de la Ley Modelo de CNUDMI se estipula que "Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria."

3.6.1 Presunción de Validez

Tal como estudiamos en el Segundo Capítulo, la firma electrónica de clave pública goza de la atribución *juris tantum*, es decir, que es el resultado del propio derecho, en lo cual no acepta prueba en contrario, siempre que cumpla a cabalidad con los preceptos legales de generación, emisión y verificación por parte de una Entidad de Certificación Acreditada.

Esta facultad ha sido recogida dentro de la Ley 67 (Art. 53), señalando que se presumirá la validez probatoria de una firma electrónica y de los datos enviados a través de ella, cuando ésta sea certificada por la respectiva EC Acreditada; dando como resultado que el firmante que ha actuado conforme a Derecho, no deberá probar los hechos controvertidos, ya que su validez se presume conforme a la Ley (Código de Procedimiento Civil, Art. 114).

3.6.2 Valoración de la Prueba

Como ya sabemos, los mensajes de datos tienen el mismo valor jurídico que los documentos físicos; es por esto que la valoración será acorde a las instrucciones establecidas en el CPC, es decir que el Juez tendrá la obligación de apreciar los mensajes de datos presentados como prueba según las reglas de la sana crítica.

En relación a lo dicho, incluido en el articulado del Reglamento General se establece que la verificación de procedencia e identidad de un mensaje de datos con su emisor se efectuará evidenciando la información contenida dentro del certificado de firma electrónica y la vigencia del mismo.

4. SERVICIOS RELACIONADOS

De manera conjunta a todos los actos y transacciones legales y comerciales que podemos efectuar por medio de la firma electrónica, existen ciertos servicios que se pueden solicitar y actividades que estamos facultados de realizar, las cuales facilitarán nuestras relaciones.

4.1 Factura Electrónica

Con la evolución computacional, la mayoría de las empresas y compañías han decidido utilizar programas informáticos para su manejo contable, donde digitalmente incluyen sus ingresos y egresos, así como la formación de archivos digitales donde constan facturas de clientes y proveedores. Pero inevitablemente estas personas jurídicas deben mantener archivos físicos de esta información, para el cumplimiento legal de registros contables y auditorías, con lo cual se crean costos de almacenamiento, problemas de legibilidad en razón de su antigüedad, tomando en cuenta la amenaza de un posible incendio o humedad que destruya o deteriore los documentos.

Pero gracias a las nuevas tecnologías y las garantías que estas presentan, se ha creado la *Factura Electrónica*, esta herramienta consiste en un método de facturación cuyo soporte ya no es físico si no electrónico, la misma que está siendo utilizado en varios países.

Su funcionamiento es el mismo que la facturación en papel, rigiéndose por las leyes tributarias de cada Estado, donde la ONU previendo los posibles conflictos entre

legislaciones, ha publicado recomendaciones en los modelos y requisitos de facturación electrónica; tal es el caso del *UNeDocs*, el cual establece los parámetros de emisión[50].

Algunos de los beneficios que tenemos con la *e-factura* son:

- Reducción en los costos de papelería y almacenamiento.
- Facilidad en los procesos contables y de auditoría.
- Impulsa el comercio internacional.
- Reduce los riesgos de falsificación y aumenta la protección de la información.
- Agilita la localización de documentos.
- Aumenta la competitividad de pequeñas y medianas empresas.

En el Ecuador esta herramienta aún no se encuentra normada, por lo que su aplicación es nula, pero solo será cuestión de tiempo para su implementación ya que dentro de las disposiciones generales de la Ley 67 se encuentra definida como el conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios. A más de ello, la Corporación Ecuatoriana de Comercio Electrónico *CORPACE*, ha elaborado un Proyecto Piloto para su implementación en el país, el cual ha sido expuesto en sedes internacionales, dando como resultado una gran aceptación. Aquello sucedió en octubre de 2008 en el Sistema Económico Latinoamericano y del Caribe *SELA*, celebrado en Venezuela.

4.2 Sellado de Tiempo

El sellado de tiempo o *Timestamping*, constituye un servicio brindado por las Entidades de Certificación Acreditada, el cual consiste en una anotación electrónica agregada a un mensaje de datos donde como mínimo incluirá la hora y fecha de emisión.

Esta prestación es de gran utilidad en casos de licitaciones, adjudicaciones, registros de propiedad intelectual, voto electrónico o notificaciones judiciales ya que al existir una certificación que estipule el día y hora exacta de la emisión del mensaje, será innegable el cumplimiento de plazos y términos o la exactitud en adjudicaciones para el primer remitente.

Dentro del Reglamento General a la Ley 67 (Art. 23) señala que para efectuar el sellado de tiempo, el emisor deberá enviar el mensaje de datos a la Entidad de Certificación para que

[50] http://www.unece.org/etrades/unedocs/

sea ésta quien remita el mensaje al receptor con la debida anotación de la hora y fecha de envío.

4.3 Notificaciones Electrónicas

Inmersa a la actividad judicial, es inevitable admitir la existencia de falencias que retrasan y desprestigian el proceso. Un ejemplo de ello son las notificaciones por parte del Juez o Tribunal hacia las partes, que en razón de descuido o impericia de sus funcionarios, éstas son retrasadas y algunas veces no cumplidas, produciendo un perjuicio para los litigantes, ya que los términos y plazos corren desde el momento de emisión de la boleta.

Afortunadamente la firma electrónica también puede ser utilizada en este campo, donde tanto el Juzgado como los actuarios legales poseerán una firma electrónica con la cual podrán recibir sus notificaciones y enviar tanto escrito sea necesario.

Se debe tomar en cuenta la disposición contemplada el Código de Procedimiento Civil, donde en su artículo 305 establece que "todos los términos se cuentan desde que se hizo la última citación o notificación; han de ser completos y correrán, además hasta la *media noche del último día*…" Es aquí donde los usuarios se preguntan ¿cómo hago efectivo este derecho, si el Palacio de Justicia solo trabaja hasta las seis de la tarde? Es cierto que podríamos ingresarlo a través de la Comisaría de turno, pero ¿esto no constituye un inconveniente para el usuario, el cual busca una administración eficaz?

En razón de esto, la firma electrónica dentro de los procesos judiciales, a más de ser un servicio complementario debe establecerse como una necesidad.

La firma electrónica sumada a la notificación electrónica y al sellado de tiempo, dan como resultado el conjunto perfecto para una comunicación segura y eficiente entre las partes y Juzgados o Tribunales dentro de un proceso judicial, esto en razón de los elementos de seguridad, identificación y no repudio que brinda la firma electrónica; la comunicación informática entre los intervinientes procesales que presta la notificación electrónica; y, la fecha y hora exacta de envió y recepción plasmada en un certificado electrónico gracias al servicio de sellado de tiempo.

Incluida en nuestra Ley 67 (Art. 56) se encuentra la siguiente disposición "Todo el que fuere parte de un procedimiento judicial, designará el lugar en que ha de ser notificado, que no puede ser otro que el casillero judicial y/o el domicilio judicial electrónico en un correo electrónico, de un abogado legalmente inscrito…" A pesar de que la normativa existe,

nuestra realidad es distinta, por cuanto la estructura técnica necesaria por parte de la Función Judicial no se encuentra ni como proyecto a mediano plazo, salvo por una pequeña iniciativa por parte del Departamento de Informática de Pichincha de la Función Judicial para la elaboración de un proyecto de inclusión del sistema.

Es necesario, antes de dar este avance, solucionar los problemas ya existentes en la actualidad, ya que si no erradicamos la corrupción e inculquemos responsabilidad a nuestros funcionarios, de nada nos servirá tener todos los medios tecnológicos para una administración de justicia eficiente.

4.4 Notario Electrónico

La figura del escribano, fedatario o notario data prácticamente desde el surgimiento del Derecho como ciencia, sus funciones de forma básica radican en brindar fe y validez pública de todo acto o contrato suscitado entre sujetos de derecho.

Con el surgimiento del comercio electrónico, su rol tomó un papel importante para la validez en la celebración de un acto o contrato por medios informáticos, surgiendo así la figura del notario electrónico o *cybernotario*.

Es cierto que para una parte de las convenciones entre particulares no es necesaria la intervención de un notario, pero ¿Qué pasa en aquellas que requieren dicha formalidad? Dentro de la compraventa de un inmueble, de una declaración juramentada, para la información sumaria, para la elaboración de ciertos testamentos, etc., constituye requisito de validez, elevar a escritura pública el acto jurídico, tanto en el mundo físico como en el telemático.

El extender los campos de aplicación del comercio electrónico constituye uno de los objetivos fundamentales de la globalización y para ello el cybernotario es pieza clave, quien será la persona encargada de dotar el reconocimiento legal de aquellos actos requirentes de solemnidad.

Ahora bien, las funciones que deben cumplir los cybernotarios son las mismas que aquellas de los notarios comunes, "son en sí mismos el sustento de legalidad de los procesos de certificación digital y tiene la posibilidad de trasladar al mundo virtual el valor de la fe pública que ejercen en el mundo real."[51]

[51] REYES KRAFFT Alfredo; *La firma electrónica…*; p. 199

La mayor parte de doctrinarios, quienes dentro de su realidad jurídica territorial han implementado esta figura, consideran como el sujeto cabal para ejercer las actividades de notario electrónico al ente certificador, ya que finalmente la función primordial de ambos es el de dar reconocimiento legal de un determinado hecho.

Finalmente considero que para el Ecuador, la reglamentación del notario electrónico debe ser el paso inmediato en nuestra legislación, por cuanto los actos jurídicos de mayor importancia requieren de intervención notarial. A más de lo dicho, se debe tomar en cuenta que la capacitación intelectual y la implementación de infraestructura técnica podrían constar como requisito para la postulación de esta dignidad, deslindando ese gasto del presupuesto estatal.

CAPÍTULO V
CONSIDERACIONES FINALES

A lo largo de la ejecución del presente trabajo he procurado destinar todos mis esfuerzos a la construcción de un instrumento que reúna de forma íntegra los elementos, funciones, definiciones, sujetos, así como la tipicidad jurídica que se encuentra inmersa dentro del profundo campo de la firma electrónica, donde el punto de partida fue el nacimiento de la escritura en la humanidad, para en definitiva concluir con los últimos avances técnicos y jurídicos, que rigen la actividad propia de los intervinientes en la estructura funcional.

En razón de esto, creo necesario y de fundamental importancia hacer una enunciación destinada a los beneficios y problemáticas que abarca la firma electrónica, introduciendo ciertas recomendaciones para la solución y posterior aplicación efectiva, y así sellar este texto con conclusiones concernientes al tema.

1. VENTAJAS DE LA FIRMA ELECTRÓNICA

Prácticamente desde las primeras páginas se ha venido describiendo las bondades y caracteres favorables que contiene la aplicación de la firma electrónica dentro de los actos jurídicos y comerciales entre las personas. No cabe duda que el dinamismo, conjugado con la seguridad que nos otorga constituye *aparentemente* (utilizo este calificativo motivado en las desventajas descritas posteriormente) el medio más fiable en nuestras interrelaciones.

A continuación presento una enumeración de los atributos más destacables del ejercicio de la autenticación digital de autoría:

- *Identificación de origen*; se convierte de manera indudable la determinación de autoría del texto recibido, una vez cumplida la verificación correspondiente del digesto y la certificación de vinculo sujeto-firma otorgada por la entidad certificante.
- *Inalterabilidad documental*; a través de la criptografía y función hash se convierte en una tarea prácticamente imposible el duplicar o alterar el mensaje enviado, ya que cualquier modificación, por ínfima que esta sea, será detectada y notificada inmediatamente.

- *Imposibilidad de desconocimiento*; al existir un nexo jurídico entre la persona con su clave, donde se incluye responsabilidad legal de las operación que se efectúen por medio de ella, queda inhabilitado el titular, a cualquier tipo de repudio ulterior, respecto a la información enviada. Cabe destacar, que de suscitarse algún siniestro que comprometa el buen uso de su clave, el titular tiene la obligación de prevenir del acontecimiento a la Entidad de Certificación, a fin de que esta proceda a la cancelación de los certificados de firma electrónica, impidiendo de tal manera su mal uso.
- *Confidencialidad*; por cuanto los métodos criptográficos que se utilizan en la transmisión de mensajes solo permiten el envío y recepción de información a las personas autorizadas, queda fehacientemente establecida la reserva de los documentos remitidos.
- *Ratificación de la recepción*; al igual que el emisor no puede negar el envío de mensajes provenientes de su clave privada, tampoco el receptor podrá desacreditar el hecho de haber acogido el documento.
- *Determinación de tiempo de envío*; queda supedita al hecho de que la Entidad de Certificación, al momento de emitir el certificado correspondiente, establezca de manera expresa la vigencia de él, con el objeto de delimitar la vida útil del mismo. Dentro de esta misma atribución se puede incluir el servicio de *sellado de tiempo*, facilitando la hora exacta de emisión, lo cual es de gran utilidad en los supuestos de acreditación o notificación para verificar el cumplimiento de términos y plazos.
- *Respaldo institucional*; con la existencia de las Entidades de Certificación, las cuales constituyen un tercero de confianza y fedatario, queda validada la firma electrónica de un sujeto, lo cual es respaldado en el certificado que éstas expiden.
- *Celeridad*; dentro de las transacciones comunes del hombre siempre existen como barreras, la eficiencia operacional y las distancias físicas entre las partes, pero con el surgimiento del Internet en conexión con la firma digital, se ha creado una vía por la cual se simplifican los actos, con un soporte legal que asegura el cumplimiento cabal de las obligaciones inmersas.
- *Derrocamiento de fronteras*; en concordancia con lo anterior, las trechos territoriales ya no componen un inconveniente entre las personas, permitiendo así la creación de vínculos fructíferos entre Estados diversos.
- *Desconocimiento de claves*; si bien la clave privada se encuentra en posesión de su titular (en el caso de criptografía asimétrica), esto no involucra el conocimiento de la misma, deviniendo así a que su divulgación es inaplicable. Es por esta razón que el

titular debe asegurarse que el dispositivo que contiene la clave no caiga en manos de terceros, que pudieren hacer uso malicioso de la misma.

2. DESVENTAJAS DE LA FIRMA ELECTRÓNICA

Es necesario considerar que en todo mecanismo, proceso, elaboración o actividad que desarrollemos, van ha existir desventajas que nos hagan dudar de su efectividad, por ejemplo en las tarjetas de crédito siempre habrá el peligro de ser clonadas, lo cual representaría un perjuicio inmenso a nuestro capital; así mismo nuestros cheques personales pueden ser falsificados o nuestras propias firmas; de igual forma, cuando creemos que el lugar mas seguro para depositar nuestro dinero es el banco, pero de manera inevitable existe la posibilidad de un *crack* financiero que de como resultado el cierre de la entidad con nuestro dinero adentro.

De similar manera existen desventajas dentro del proceso de firma electrónica, pero lo importante aquí es poner en una balanza los beneficios y problemas, para demostrar que por más que existan amenazas de un perjuicio, siempre prevalecerán los hechos favorables y que lo negativo abarca un porcentaje mínimo, el cual puede ser superado con la correcta aplicación de metodología y la implementación acertada de normativa jurídica.

Ahora bien, dejemos de lado las justificaciones y pasemos a enumerar lo negativo de la firma electrónica:

- En primera instancia, podemos establecer como barrera inicial el *impacto psicológico en el hombre*. Desde los tiempos inmemoriales de la escritura, el único soporte que existía era el físico, el material, aquel constante por átomos, es por esto que siempre vendrá la idea de que algo es real cuando lo podemos palpar y que las obligaciones legales únicamente se crean plasmando nuestra firma en un papel. Afortunadamente, solo es cuestión de tiempo para que las personas se acostumbren a la utilización de la informática y con la práctica se logre entender sus beneficios y eficacia.
- *Heterogeneidad legislativa*; dentro del marco internacional radica como problema el hecho de que cada Estado posea su propia normativa y parámetros de aplicación, siendo en algunos tan restrictivas que los hacen incompatibles con el resto. Por ejemplo mientras en algunas naciones se reconoce cualquier método criptográfico, en otros los delimitan de manera excluyente.

- *Posibilidad de ser craqueados*; los medios de seguridad siempre irán en ascenso de forma paralela a la evolución informática, pero la amenaza de violación a estas seguridades es latente. Los hackers dedican su tiempo ha buscar falencias en estos sistemas, pero no solo son ellos los posibles infractores, el solo hecho de dejar nuestra computadora prendida puede dar como resultado que un tercero tenga acceso a nuestra clave privada y por lo tanto haga un mal uso de ella; por otra parte debemos tomar en cuenta la posibilidad de que nuestro computador requiera ser reparado por un técnico, dando como resultado que toda nuestra información se encuentre en sus manos.
- *Limitación de transacciones*; el ámbito de aplicación que se puede dar a la firma electrónica varia de una legislación a otra, ya que a diferencia del Ecuador, no todos los Estados dejan la puerta abierta para la realización de transacciones de cualquier tipo.
- *Ámbito geográfico*; lamentablemente no todas las naciones aceptan las firmas electrónicas de todos los demás Estados. Por ejemplo, algunos países de la Comunidad Europea solo reconocen las firmas de los miembros de la Comunidad, excluyendo a los demás.
- *Mal manejo de registros*; las Entidades de Certificación tienen la obligación de mantener un registro, tanto de los titulares como de los certificados emitidos, pero esta información puede no ser exacta o no tener la actualización periódica necesaria, creando un perjuicio para los usuarios. La dirección domiciliaria o la permanencia en determinado cargo puede variar de un momento a otro, es por esto que las políticas internas de las EC así como de sus autoridades de control deben ser rigurosas y eficaces de tal manera que los márgenes de error sean mínimos.
- *Validez probatoria*; en el Capítulo anterior ya se mencionó las atribuciones legales y la fuerza probatoria que tienen los mensajes de datos en nuestro país, pero esto no es una realidad general en el mundo, por ejemplo en Grecia o Francia la validez legal de ciertos contratos versará en el hecho de que conste en un documento físico, limitando así la su aplicación.
- *Valoración de la prueba*; dentro de nuestro propio territorio, a pesar del valor probatorio que poseen los mensajes de datos, siempre estaremos a merced de la capacitación y medios de verificación que posean nuestros administradores de justicia, donde el conocimiento que ellos tengan respecto a las nuevas tecnologías será de vital importancia para la correcta aplicación de las mismas.

Como vemos, todos estos problemas y limitaciones que pueden surgir, son fácilmente subsanables, ya sea por medio de un consenso internacional donde se determine los

parámetros específicos para la aplicación y reconocimiento comunitario de la firma electrónica, o a través de reglas generales internas que planteen los requisitos mínimos de seguridad y control a fin de lograr un método altamente fiable, en el cual las personas depositen su confianza y se logre un desarrollo comercial sostenible en todas las naciones.

3. CONCLUSIONES

- Conforme ha ido evolucionando la sociedad, donde las relaciones comerciales entre personas siempre ha avanzado con el objetivo esencial de vincularse con sujetos ajenos a su territorio, en razón de la competitividad y desarrollo, la firma manuscrita ya no constituía el medio más idóneo para alcanzar estos fines por cuanto los costos y la celeridad en las transacciones se veían trabadas en razón de la distancia; pero el nacimiento del Internet fundó la herramienta adecuada para derribar fronteras y originar un medio que facilite el comercio de manera eficaz.
- Dentro del mundo globalizado que nos encontramos, se ha vuelto indispensable la utilización de medios electrónicos, donde nuestros posibles clientes, proveedores y distribuidores, ubicados en distintos puntos del globo, se encuentran a un *clic* de distancia, y debiendo además tomar en cuenta que el movimiento de capitales se ha facilitado enormemente, para así cerrar el círculo transaccional entre comerciantes.
- El Internet fue el instrumento preciso para el comercio internacional, pero con el defecto de carecer de las seguridades necesarias para los usuarios; es por esto que la firma electrónica instituye el complemento exacto para alcanzar una relación jurídica y comercial segura, donde la autoría era reconocida e innegable, armada de un marco legal que garantizaba la obligatoriedad de los convenios contraídos.
- En las diversas legislaciones y doctrinas, se hace una distinción conceptual entre firma electrónica y firma digital, donde a la segunda se le atribuye mayor seguridad y tecnicidad que involucra a la criptografía, dando como resultado la inviolabilidad de la información y el no repudio por parte de sus usuarios. A pesar de que en el Ecuador, dentro de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establece como método de aplicación a la firma electrónica, esto no obsta de la utilización de criptografía por cuanto la definición legal que se le da es amplia y suficiente, donde además se complementa con la los requerimientos técnicos y estructurales que se exigen a las Entidades de Certificación para la emisión de firmas

electrónicas, reflejando así la necesidad de métodos de seguridad vastos para sus usuarios.

- Con la creciente utilización de firmas electrónicas en las relaciones comerciales, la tipicidad de estos actos conlleva ser un requisito apremiante por cuanto su uso involucra la manifestación de voluntad del titular; en el Ecuador, este tema fue legislado por primera vez en el año 2002 con la Ley de Comercio Electrónico, a partir de esto, poco a poco se ha ido ampliando el marco jurídico con el registro de Reglamentos y Reformas relacionadas. En la actualidad, luego de seis años, se institucionalizó la primera Entidad de Certificación pública. Por el momento se desconocen los efectos y la acogida que se le de en nuestro medio, solo será cuestión tiempo, publicidad y buen manejo para que nuestro país se involucre en el progreso y desarrollo económico internacional a través de la informática.
- Nuestra legislación ha sabido englobar todos los puntos intervinientes dentro del proceso transaccional de la firma electrónica, desde la construcción de una estructura institucional completa, hasta las implicaciones jurídicas que abarca la utilización de mensajes de datos. Ahora solo dependerá de la instrucción e importancia que la administración de justicia y demás entes administrativos públicos, sepan darle para lograr una evolución sostenida de este nuevo campo.
- Empero de lo anterior, aún existen falencias y pequeños vacíos legales que se deben considerar, tal es el caso de la normativa para notario electrónico y la factura electrónica, como también la falta de publicidad al público. A pesar de ello, tengo la certeza que estos ligeros detalles serán corregidos, a fin de lograr una reglamentación completa.
- En definitiva, para lograr una aplicación global, donde ninguna nación se encuentre excluida por normativas contrapuestas, es apremiante la existencia de homogeneidad legislativa mundial, donde los organismos internacionales como la ONU, UE, CAN, etc., deben ser los guías y gestores para el establecimiento de parámetros generales en la aplicación de firmas electrónicas de forma universal, donde los tratados internacionales se constituirían en los portadores de obligatoriedad para el cumplimiento cabal entre Estados.

BIBLIOGRAFÍA

- **ALTERINI**, Atilio A., 1998, *Contratos civiles, comerciales, de consumo. Teoría General*, Ed. Abeledo Perrot, Buenos Aires - Argentina.
- **BRIZZIO**, Claudia R., 2000, *La informática en el nuevo derecho*, Ed. Abeledo Perrot, Buenos Aires - Argentina.
- **CHIOVENDA**, Giuseppe, 1940, *Instituciones de Derecho Procesal Civil*; Revista de Derecho Privado, Madrid - España.
- **DEVOTO**, Mauricio, 2001, *Comercio Electrónico y Firma Digital*, Ed. La Ley, Buenos Aires – Argentina.
- **HERRMANN**, Patricia, 2007, *Comercio Electrónico*, Ed. Universidad Técnica Particular de Loja, Loja – Ecuador.
- **HOCSMAN** Heriberto Simón, 2005, *Negocios en Internet*, Ed. Astrea, Buenos Aires – Argentina.
- **LORENZETTI**, Ricardo Luis, 2002, *Comercio Electrónico*, Ed. Abeledo Perrot, Buenos Aires - Argentina.
- **MARTÍNEZ** Nadal, Apolonia, 2000, *Comercio electrónico, firma digital y autoridades de certificación*, Ed. Colección Estudios de Derecho Mercantil Civitas, Madrid – España.
- **SALGADO** Pesantes, Hernán, 2006, *Lecciones de derecho constitucional*, Ed. Ediciones Legales, Quito – Ecuador.
- **SARRA**, Andrea Viviana, 2001, *Comercio electrónico y derecho*, Ed. Astrea, Buenos Aires - Argentina.
- **PÁEZ** Rivadeneira Juan José, 2005, *Manual de Firmas Electrónicas y Mensajes de Datos*, Ed. Corporación De Estudios y Publicaciones, Quito - Ecuador.
- **R.O. 147,** ECUADOR, *Código Penal*, 22 de enero de 1971, Quito – Ecuador.
- **R.O. 320**, ECUADOR, *Ley de Propiedad Intelectual*, 19 de mayo de 1998, Quito – Ecuador.
- **R.O. 536**, ECUADOR, *Ley del Régimen Jurídico Administrativo de la Función Ejecutiva*, 18 de marzo de 2002, Quito – Ecuador.

- **R.O. 557**, ECUADOR, *Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos*, 17 de abril de 2002, Quito – Ecuador.
- **R.O. 735,** ECUADOR, *Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos*, 31 de diciembre de 2002, Quito – Ecuador.
- **R.O. 58,** ECUADOR, *Código de Procedimiento Civil*, 12 de julio de 2005, Quito – Ecuador.
- **R.O. 449**, ECUADOR, *Constitución Política*, 20 de octubre de 2008, Quito – Ecuador.
- **Res. 584-23-2003**, CONATEL.
- **Res. 324-17-2006,** CONATEL.
- **Res. 454-19-2006,** CONATEL.
- **Res. 456-19-2006,** CONATEL.
- **Res. 457-19-2006,** CONATEL.
- **Res. 458-19-2006,** CONATEL.
- **Res. 477-20-2008,** CONATEL.
- **Res. 478-20-2008,** CONATEL.
- **REYES** Krafft Alfredo Alejandro, 2003, *La firma electrónica y las entidades de certificación*; Ed. Porrúa, DF – México.
- **RICO** Carrillo Mariliana, 2007, *Derecho de las nuevas tecnologías*, Ed. La Roca, Buenos Aires – Argentina.
- **SERRA** Domínguez Manuel, 1969, *Estudios de Derecho Procesal*, Ed. ARIEL, Barcelona-España.

HEMEROGRAFÍA

- http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=firma
- http://europa.eu/scadplus/leg/es/lvb/l24118.htm
- http://daccessdds.un.org/doc/UNDOC/GEN/N01/490/29/PDF/N0149029.pdf?OpenElement
- http://www.itu.int/ITU-D/cyb/publications/archive/Legislacion%20Comercio%20Electronico%20CAN1.pdf
- http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf
- www.law.miami.edu/~froomkin/articles/trusted1.htm
- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:ES:HTML
- http://www.conatel.gov.ec/site_conatel/index.php?option=com_content&view=article&id=371:resoluciones-octubre-diciembre-2008&catid=134:resoluciones-2008&Itemid=201
- http://www.zur2.com/objetivos/leyextran/cnudmi.htm
- http://www.unece.org/etrades/unedocs/