

**TRATAMIENTO LEGAL COLOMBIANO DE LA FIRMA ELECTRÓNICA PARA
EL DESARROLLO DEL COMERCIO ELECTRÓNICO**

**MAURICIO GARCÍA ARBOLEDA
SEBASTIÁN GIRALDO CASTAÑEDA
ÁNGELA MARÍA RESTREPO GÓMEZ**

**PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE CIENCIAS JURÍDICAS
ESPECIALIZACIÓN EN DERECHO COMERCIAL
BOGOTÁ D.C
2013**

**TRATAMIENTO LEGAL COLOMBIANO DE LA FIRMA ELECTRÓNICA PARA
EL DESARROLLO DEL COMERCIO ELECTRÓNICO**

**MAURICIO GARCÍA ARBOLEDA
SEBASTIÁN GIRALDO CASTAÑEDA
ÁNGELA MARÍA RESTREPO GÓMEZ**

**HERNÁN DARÍO SANTANA FERRIN
Director de Tesis**

**Trabajo de Grado para obtener el título de:
ESPECIALISTA EN DERECHO COMERCIAL**

**PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE CIENCIAS JURÍDICAS
ESPECIALIZACIÓN EN DERECHO COMERCIAL
BOGOTÁ D.C
2013**

NOTA DE ADVERTENCIA

“La Universidad no se hace responsable por los conceptos emitidos por sus alumnos en sus trabajos de tesis. Solo velará por que no se publique nada contrario al dogma y a la moral católica y porque las tesis no contengan ataques personales contra persona alguna, antes bien se vea en ellas el anhelo de buscar la verdad y la justicia”.

CONTENIDO

I. LA LEY DE COMERCIO ELECTRÓNICO FRENTE AL COMERCIO ELECTRÓNICO ACTUAL: MARCO NORMATIVO.....	12
II. CONCEPTO DE EQUIVALENTE FUNCIONAL (ARTÍCULO 7 DE LA LEY 527 DE 1999)	21
a. Equivalente funcional de escrito.	28
b. Equivalente funcional de firma.....	29
c. Equivalente funcional de original.....	33
d. Equivalente funcional de archivo y conservación.	35
III. EL CÓDIGO GENERAL DEL PROCESO Y LA PRESUNCIÓN DE AUTENTICIDAD DE LOS MENSAJES DE DATOS: MODIFICACIÓN A LA LEY DE COMERCIO ELECTRÓNICO.	38
3.1. Noción de mensaje de datos desarrollada por la Ley 527 de 1999.....	38
3.2. Problemática de la Ley de Comercio Electrónico frente a los mensajes de datos: regulación excesiva y tratamiento preferencial de la firma digital.....	40
3.3. El Código General del Proceso y la presunción de autenticidad de los mensajes de datos.	48
IV. ENTIDADES DE CERTIFICACIÓN.	51
4.1. Requisitos de las entidades de certificación.	53
V. EL TRATADO DE LIBRE COMERCIO SUSCRITO ENTRE ESTADOS UNIDOS Y COLOMBIA Y SU INCIDENCIA EN LA LEGISLACIÓN SOBRE COMERCIO ELECTRÓNICO.	59
5.1. El Decreto 2364 de 2012 y la armonización del principio de equivalencia funcional plasmado en el artículo 7 de la Ley 527 de 1999.....	60
5.2. El Decreto 19 de 2012 y la facultad de certificar firmas electrónicas.	64
VI. LA CONTRATACIÓN ELECTRÓNICA.....	69
6.1. El consentimiento electrónico, la oferta y su aceptación.....	72
VII. CONCLUSIONES.....	78
VIII.BIBLIOGRAFÍA.....	81

I. LA LEY DE COMERCIO ELECTRÓNICO FRENTE AL COMERCIO ELECTRÓNICO ACTUAL: MARCO NORMATIVO.

El comercio electrónico a través de los tiempos ha venido cobrando mayor importancia dado que los avances tecnológicos que se han presentando en el transcurso de los años, avances tecnológicos de los que las personas con el pasar de los días dependen cada vez más para el desarrollo de sus actividades, toda vez que las relaciones jurídicas de hoy en día han venido implementando sistemas informáticos y por lo tanto estas dependerán de los mecanismos actuales, de igual manera la tecnología cada vez tiene un mayor impacto en la economía del mundo, trayendo esto implicaciones en el ámbito jurídico, que han llevado sin lugar a dudas a la implementación de una regulación al respecto, de esta manera se trae a colación que en los primeros momentos de creación de normas jurídicas sobre el comercio electrónico, se establecieron algunos presupuestos por medio de los cuales se facilita tal implementación de las nuevas tecnologías en las relaciones jurídicas contemporáneas, a saber:

- *“Las partes deberían tener la mayor libertad para establecer la relación contractual que más les conviniera.*
- *Las normas debían ser tecnológicamente neutras y orientadas hacia el futuro, es decir, no debían convertirse en un obstáculo para el uso o creación de nuevas tecnologías.*
- *La modificación de las normas vigentes o la adopción de nuevas normas solo debía hacerse cuando fuera necesario, para apoyar el uso de nuevas tecnologías.*
- *En el proceso de creación de normas aplicadas a nuevas tecnologías debía participar el sector comercial de alta tecnología, así como las empresas o entidades gubernamentales que no se hubieran incorporado a las nuevas tecnologías y que*

requerían de procesos de modernización, para reorientar sus procesos y organizaciones¹”.

De acuerdo a lo anterior, en la actualidad, una regulación del comercio electrónico requiere necesariamente asentarse sobre un concepto amplio y moderno que permita que se puedan configurar las relaciones entre las personas, por lo que se debe apartar de los parámetros tradicionales , y por lo tanto permitirá la incorporación de nuevas características que se adapten a la nueva realidad, de esta manera es claro que el legislador a través de la Ley de Comercio Electrónico que es objeto del presente escrito propendió por implementar un sistema que brindara la seguridad jurídica necesaria a la utilización de nuevos sistemas en los que se plasma la voluntad; dentro de las características arriba señaladas se debe incluir, que las operaciones de comercio puedan ser realizadas vía electrónica o digital, esto es por medio de mensajes de datos, a fin que se pueda desarrollar este tipo de comercio sin tener en cuenta el lugar de ubicación de las partes, dado que ello se torna irrelevante en este tipo de comercio y en las nuevas relaciones comerciales de hoy en día; así las cosas, en principio no queda una constancia como tal del acuerdo en un papel propiamente dicho, se genera un código mediante el que las partes intervinientes pueden acceder a la información plasmada en un mensaje de datos, situación que genera una disminución de intermediarios y cada empresa o comerciante por pequeño que sea en el mercado puede llegar a tener un acceso mundial², ya que se tiene un sistema reconocido para brindar la seguridad requerida y por lo tanto intermediarios que se encargaban de verificar la autenticidad de un documento quedan por fuera de la relación jurídica que se contruye, es por esto, que el comercio electrónico trae grandes beneficios en el comercio ya que de una u otra manera genera agilidad y eficiencia en el mercado.

Ahora bien, es de anotar que un documento por medio del que se expresa la voluntad de cada uno de los contratantes y/o partes, bien sea por medio de un papel físico o de un mensaje de datos, sirva para corroborar la manifestación en el mismo plasmada, sin

¹ RINCÓN CÁRDENAS, Erick. *“Manual de Derecho de Comercio Electrónico y de Internet”*, Ed. Universidad del Rosario. Bogotá, 2006. Pág. 22

² Cfr. Ibíd. Pág. 24

embargo el diccionario de la Real Academia Española ha definido al documento como un *“Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo”*; por su parte el mensaje de datos, como elemento fundamental del comercio electrónico, ha sido entendido de acuerdo con el literal (a) del artículo 2 de la ley 527 de 1999 como *“la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax”*, por lo que podemos concluir en términos generales que, con la regulación del comercio electrónico se propende porque el mensaje de datos pueda ser tomado como equivalente a un documento físico y tradicional, aspecto sobre el cual la Certicámara señaló que la idea del comercio electrónico es lograr que el documento electrónico se equipare al documento manuscrito, llegando estos dos a tener los mismos efectos probatorios, y así cuando se requiera que un documento conste por escrito bastaría con un mensaje de datos.³, por lo que al cumplir las mismas funciones, podemos empezar a reemplazar o implementar los mecanismos alternos que están consagrados en la ley, bien sea mediante documento propiamente dicho o por un mensaje de datos, puesto que estos instrumentos gozan de los mismos efectos jurídicos, tema que será tratado a profundidad más adelante.

Una vez analizada la situación general respecto del comercio electrónico, es preciso analizar este tema en Colombia, para lo que se encuentra que actualmente se encuentra vigente la Ley 527 de 1999, por medio de la que se dan los primeros lineamientos respecto al Comercio Electrónico en el país, y aunque no es el único asunto que trata, esta norma se ha creado en virtud del cambio tecnológico que se ha venido presentado en el mundo y por lo tanto debido a que el legislador se ha visto en la necesidad de responder a las nuevas exigencias y requerimientos que el mundo moderno trae una vez comprendidas estas nuevas tecnologías, es decir, el mundo jurídico debe acoplarse a las nuevas formas como los comerciantes y/o ciudadanos del común se encuentran negociando sus relaciones jurídicas, por lo que la legislación no se puede ver rezagada con respecto a las nuevas tecnologías, de esta manera deben adecuarse los ordenamientos jurídicos.

³ Cfr. Fuente de Internet, Documento de la Certicámara S.A
<http://web.certicamara.com/media/69109/validez%20y%20seguridad.pdf>

Conforme lo anterior, es indispensable tener presente la exposición de motivos que dio origen a la ley, toda vez que la misma permite conocer las razones por las que se expidió la misma, de esta manera, es claro que tanto el Congreso de la República como los Ministros de Justicia y del Derecho, de Desarrollo, de Comercio Exterior y de Transporte, argumentaron la necesidad de implementar una normatividad que estuviere conforme a las nuevas realidades y que le diera fundamento jurídico a las transacciones comerciales realizadas por medios electrónicos, así en este proyecto de ley se estableció:

“El desarrollo tecnológico que se viene logrando en los países industrializados, permite agilizar y hacer mucho más operante la prestación de los servicios y el intercambio de bienes tangibles o intangibles, lo cual hace importante que nuestro país incorpore dentro de su estructura legal, normas que faciliten las condiciones para acceder a canales eficientes de derecho mercantil internacional, en virtud a los obstáculos que para éste encarna una deficiente y obsoleta regulación al respecto”⁴.

Igualmente, se evidencia que en el proyecto de ley 227 de 1998 se señaló que el mismo tenía por objetivo *“brindar un adecuado tratamiento al contenido de las comunicaciones, denominado intercambio electrónico de información, o según sus siglas en ingles, EDI, aunque no dejaba de lado otros medios de comunicación de datos. Además se centraba en el aspecto probatorio, habida cuenta de que en el futuro la información presentada por estos medios sería distinta a la noción tradicional que se tiene de documento”*⁵, de esta manera, es claro que desde momentos previos a la expedición de la ley objeto del presente documento, ya se venía tocando el tratamiento de las nuevas comunicaciones para la implementación de sistemas veraces y acordes a la realidad de las necesidades del mercado.

No hay que perder de vista, que La ley 527 de 1999 tomó como base la ley modelo sobre comercio electrónico de la Comisión de las Naciones Unidas para el desarrollo del derecho mercantil internacional (CNUDMI), ley que se inspiró en el propósito de dar un respaldo

⁴ Corte Constitucional. Sentencia C-662 de 2000. M.P. Alejandro Martínez Caballero.

⁵ RINCÓN CÁRDENAS, Erick. *“Manual de Derecho de Comercio Electrónico y de Internet”*, Ed. Universidad del Rosario. Bogotá, 2006. Pág. 30

jurídico al comercio electrónico que se venía presentando y brindar un mayor impulso a este para lograr su expansión.

Es menester manifestar que la ley modelo, así mismo, tomó como base la Resolución 51 de 1996 creada por la Asamblea General de la ONU, la cual aprobó la ley modelo sobre comercio electrónico y generó recomendaciones para que la misma fuera incluida en los diferentes ordenamientos internos, buscándose con esto un punto de partida para que diferentes países pudieran aplicar nuevas técnicas tecnológicas y así facilitar el comercio. Esta ley, estableció que la misma sería aplicable a todo tipo de información mediante mensaje de datos y especificó su campo de acción a las actividades comerciales, posteriormente determinó como debía ser interpretado el término “comercial”, indicando en términos generales que por este término debía entenderse toda relación que tuviere un carácter comercial, tuviera esta o no un origen contractual.

En igual sentido, como antecedentes al comercio electrónico, propiamente dicho, encontramos como referencia de medios electrónicos utilizados, el numeral 6, del artículo 127 del Decreto 663 de 1993, que disponía que para el pago de depósitos de ahorro era necesario libreta u otra constancia del depósito, salvo que el usuario utilizara un medio electrónico que permitiera dejar evidencia fidedigna de la transacción realizada; de igual manera el artículo 139 hacía referencia a las Corporaciones de Ahorro y Vivienda para que cobraran por los servicios prestados por medio de los sistemas electrónicos de depósito y retiro. Así mismo el artículo 26 del Decreto 2150 de 1995 ordenaba a las entidades públicas la habilitación de sistemas de transmisión electrónica de datos, para que los usuarios logaran una comunicación efectiva con estas. Por lo que resulta claro que los sistemas de comunicación de datos via electrónica no ha estado fuera del interés del legislador, puesto que desde hace más de quince (15) años se ha venido regulando parcialmente la materia.

Ahora bien, se puede decir más exactamente, en lo referente a los antecedentes internacionales que los primeros visos del uso de tecnologías en el intercambio se dio en las actividades militares a finales de los años setenta, cuando en Estados Unidos se inicia un programa de investigación para intercambiar información entre diferentes redes de computadores, pero como tal la primera expresión del comercio electrónico se dio con el

Intercambio Electrónico de Informaciones o el EDI (Electronic Data Interchange), el EDI se encuentra dirigido a empresarios y es un “*intercambio electrónico de datos de computadora a computadora entre Socios Comerciales (cadenas), con la finalidad de ahorrar tiempo al eliminar los tradicionales métodos de preparación y envío de documentos a través de mensajería. A la vez, tiene la ventaja de ser un método más seguro y confiable para el manejo de información*”⁶.

Así las cosas, la Ley 527 de 1999 es clara en señalar y determinar que la misma sería aplicable a todo tipo de información que se plasme en un mensaje de datos, por lo que estableció en su artículo primero su ámbito de aplicación de la siguiente manera:

“La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

- a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;*
- b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo”.*

Para un mayor entendimiento la ya mencionada norma se encargó de definir el comercio electrónico en los siguientes términos:

“Comercio electrónico. Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas

⁶ Fuente Internet. <http://www.masteredi.com.mx/SP/INFORMACION/que.asp>

de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.”

Conforme tal definición, es clara la voluntad del legislador en la implementación de nuevos sistemas jurídicos que se adecuaran a las necesidades tecnológicas que fueran surgiendo, tanto así que se identifica y otorga plena validez a todos aquellos actos que sean realizados mediante la manifestación de la información mediante unos mensajes de datos, de esta manera la legislación colombiana se flexibiliza en cuanto a los requisitos que se exigen para brindar plenos efectos al mismo.

Por su parte, la ley Colombiana, es de recordar que tuvo como inspiración la normatividad de las Naciones Unidas tal como se evidenció líneas arriba, en aras de brindar al sistema legal colombiano la agilidad que el mercado demanda para la celebración de negocios jurídicos, sin embargo tal normatividad busco ir más allá de una simple transcripción de la norma ultranacional que sirvió para expedir la norma local, toda vez que no solo incluyó regulación respecto de los mensajes de datos, su validez y efectos jurídicos (probatorios), sino que adicionalmente reguló y creó a las entidades de certificación, los certificados digitales y las firmas digitales, con los que se garantiza que haya una tercera persona que en principio es imparcial ante las partes involucradas y de esta manera se aporta una mayor seguridad jurídica a este sistema y relaciones que se encuentra implementándose gracias a la flexibilidad que trae la ley objeto de estudio, sin embargo estos asuntos serán expuestos en capítulos siguientes. De esta manera, la ley 527 de 1999 impulsada por el Ministerio de Justicia con participación de los Ministerios de Comercio Exterior, Transporte y Desarrollo y con colaboración tanto del sector público como del privado, puso la normatividad Colombiana al nivel de las nuevas tendencias de derecho internacional para llenar aquellos vacíos que se venían presentando en las nuevas modalidades de contratación utilizadas por los comerciantes para agilizar la celebración de tales negocios, así esta ley se ha distribuido en 3 grandes acápites: a) Transporte de mercancías b); firmas digitales, certificados y entidades de certificación c) reglamentación y vigencia, por lo que es clara la intención del legislador respecto a la importancia que se da a las nuevas relaciones comerciales que surgen como consecuencia de las nuevas tecnologías, es por ello que se brinda desde la

óptica jurídica una validez a aquellas firmas digitales y se implementan terceros neutrales que se encarguen de reconocer tales actuaciones.

Así mismo, dentro de la ley 527 de 1999 se incorporaron una serie de principios encargados de regir el comercio electrónico, dentro de los cuales se incluye:

- **Equivalencia funcional de los actos electrónicos.** Como principio rector, se encarga de indicar que la instrumentación electrónica cumple la misma función y tiene la misma validez de la instrumentación escrita u oral, por lo cual los mensajes de datos deben recibir el mismo tratamiento.
- **Neutralidad Tecnológica.** Consistente en que las normas no solo abarquen las tecnologías que dieron origen a su reglamentación sino también a las tecnologías futuras.
- **Buena fe.** Se trata simplemente de reafirmar este principio en el intercambio de bienes y servicios por medios que impliquen la utilización de medios tecnológicos.
- **Libertad Contractual.** Principio que se basa en la libertad de empresa, en la autonomía privada y en la libertad de competencia, permitiendo una libertad de configuración de la relación entre las partes siempre y cuando se respete un marco normativo.
- **No se Altera ni Modifica el Actual Régimen del Derecho de las Obligaciones y Contratos Privados.** La regulación del comercio electrónico no modifica la normatividad vigente ya que esta solo se encarga de un soporte y de una ampliación del derecho existente⁷.

No siendo suficiente la ley 527 de 1999, con posterioridad a esta y en desarrollo de la misma, en el año 2000 fue expedido el Decreto 1747 de 2000 que se encargó de dar una regulación de mayor amplitud y especificación en cuanto a las entidades de certificación y en lo referente a los certificados digitales, de esta manera el referido Decreto reglamentó parcialmente la Ley 527 de 1999 estableciendo cada uno de los requisitos que se debían

⁷ Cfr. Ibid. Págs.52 y 53.

acreditar tales entidades para poder actuar como una entidad de certificación ya sea esta abierta o cerrada dependiendo de los requisitos que se exijan para el efecto, adicionalmente se establecieron las reglas de patrimonio que se debían cumplir para poder establecerse como una entidad de certificación, las garantías que se debían acreditar, las infraestructura y los recursos con los cuales debía contar, entre otras obligaciones con las que debe cumplir una entidad para poder ser considerada como de certificación; con esto tenemos que la temática del comercio electrónico no se ha quedado con la ley 527 de 1999 sino que esta ha seguido siendo desarrollada, tomándola como un pilar pero no como la única norma sobre el tema.

II. CONCEPTO DE EQUIVALENTE FUNCIONAL (ARTÍCULO 7 DE LA LEY 527 DE 1999).

En primera medida, se debe entender por equivalente funcional como aquel principio por medio del cual se brinda un mayor espectro a aquellos instrumentos (documentos, papeles, mensajes de datos, correos electrónicos, entre otros) que se han utilizados para el desarrollo del comercio entre dos o más partes, bien sea que se encuentren en el mismo lugar o en diferente ubicación geográfica. De esta manera, es evidente que este principio sirve para dar mayor dinamismo a las relaciones contractuales en el mercado, toda vez que permite equiparar unos instrumentos no tradicionales para manifestar la voluntad de cada uno de los contratantes en la celebración de un negocio jurídico, claro está, debiendo cumplir una serie de requisitos sin los cuales, no podría “equivaler” este nuevo instrumento a las formas tradicionales de celebrar contratos, es decir, de manera escrita y en papel físico.

La equivalencia funcional permite que todo lo que sea susceptible de ser realizado por un medio físico o tradicional, pueda materializarse por medios y/o canales electrónicos, teniendo estos instrumentos los mismos efectos probatorios, es decir, un documento electrónico hace las mismas veces que un documento físico y/o tradicional, toda vez que los mismos tienen las mismas calidades y cualidades que permiten identificar el documento per se, y de esta manera es claro que un documento de papel y uno electrónico no tienen diferencia alguna, tan solo se trata del soporte en el que reposa la información, pues uno será en físico y el otro digitalmente, de esta manera no hay razón alguna por la que no sea procedente otorgar tales efectos (probatorios) a los mecanismos digitales, claro está, se requiere que el instrumento donde conste tal mensaje de datos tenga cierta seguridad que permita que el texto no sea alterado⁸.

⁸ Fuente internet: http://www.sela.org/attach/258/default/Di-7-12_Fundamentos_Firma_Digital_y_su_Estado_Arte_en_ALC-Final.pdf

Teniendo en cuenta lo anterior, es indispensable conocer el concepto de Equivalente Funcional, que particularmente se encuentra regulado en el artículo 7 de la Ley 527 de 1999, ya que si bien la norma se refiere a la *Firma*, debe entenderse que este concepto es el que trae a colación el Equivalente Funcional, toda vez que permite que cuando una firma se encuentre plasmada en un mensaje de datos o cualquier otro instrumento y cumpla los requisitos adicionales señalados en tal artículo, tendrá los mismos efectos que cualquier firma registrada en un documento en papel físico o realizada manuscritamente.

Una vez definido este concepto, es indispensable conocer el origen de la equivalencia funcional, por lo que se hará referencia a la Ley 527 de 1999 que establece el marco normativo del acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, particularmente al artículo 7 de la misma, que reza:

“ARTICULO 7o. FIRMA. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

- a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;*
- b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.*

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma”.

De esta manera, es clara la norma en señalar que la firma de cualquier mensaje de datos cuyo método sea confiable y apropiado para cumplir la finalidad del mensaje mismo, será perfectamente válido y gozará de plenos efectos jurídicos y probatorios para que se entienda que el referido mensaje de datos hace las veces de un documento físico y escrito debidamente firmado por las partes.

Así las cosas, una vez estudiado el origen y fuente del principio objeto de este capítulo, es menester proceder a explicar la funcionalidad que del mismo se deriva en el ámbito de la Ley de Comercio Electrónico, para lo que nos referiremos a la exposición de motivos de la referida Ley donde se evidencia claramente que el legislador concibió la firma de los documentos electrónicos y particularmente los mensajes de datos como aquellos instrumentos que sirven para el normal desarrollo del comercio y particularmente el comercio electrónico, esto es, son aquellos que se asemejan a la firma de cualquier documento y por lo tanto generan los mismos efectos que cualquier documento escrito y en papel, de esta manera es claro que el equivalente funcional tiene como principal función el otorgamiento de validez y efectos probatorios a cualquier firma que se plasme bien sea en un documento físico o a cualquier otro que sea digital, lo anteriormente señalado se refleja en la siguiente cita de la exposición de motivos de la Ley, así:

“en conclusión, los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplen los requisitos técnicos y jurídicos plasmados en la ley”.

En igual sentido, otros autores han venido señalando que la finalidad de la firma electrónica es brindar a los agentes de la rama judicial colombiana, herramientas que permitan juzgar la validez de un mensaje de datos, es decir, que cuando sea presentada una diferencia respecto a un mensaje de datos, pueda el juzgador partir de los requisitos consagrados en la Ley 527 de 1999 para así determinar los efectos que tenga el mismo, de esta manera el profesor Marco Pérez⁹ en su artículo “El Tratamiento Legal de la Firma Electrónica en Colombia y en el Derecho Uniforme” en la Revista e-mercatoria de 2002, señala que el principio de equivalente funcional tiene como finalidad “que los jueces o árbitros, apliquen los requisitos de la ley caso por caso sin restringir el uso de nuevas tecnologías de firma. Para cada tecnología de firma, el juez o árbitro hará una adecuación de la misma, frente a los

⁹ Investigador de la Universidad Externado de Colombia

*requisitos del artículo 7 de la Ley 527 de 1999*¹⁰, es decir, cuando el juez o árbitro se encuentre frente a un asunto de validez de una firma en un documento digital, debe acudir al artículo 7 de la referida ley para denotar si la misma presta las veces de una firma cotidiana en documento físico y en consecuencia sirva de documento en el que se plasme la voluntad de alguno de los contratantes.

Ahora bien, debe entenderse que la firma digital conlleva inexorablemente a evidenciar que la misma cuenta con un valor probatorio en el mundo jurídico colombiano en gran medida, tanto así que esta es la pretensión que trae consigo el principio de equivalencia funcional de tal instrumento, por lo tanto debe tenerse que la firma digital al ser un mecanismo fiable y ampliamente reconocido por la legislación, cuenta así mismo con la validez y el valor probatorio necesario para los mismos fines, es decir, se trata de un mecanismo que es perfectamente adecuado para la celebración de los negocios jurídicos en el mercado actual, por tal motivo, vale la pena resaltar el criterio que tiene Erick Rincón Cárdenas sobre la validez y valor probatorio de la información que se consigne en mensajes de datos, toda vez que en resumidas cuentas se debe tener que hay una igualdad entre los mensajes de datos y los demás medios de prueba mediante los que se consagre la información debidamente documentada, firmada y aceptada por las partes, y de esta manera se demuestra en la Ley de Comercio Electrónico que propende por dar un mayor dinamismo a las relaciones jurídicas que se den en el mercado, así las cosas, es indispensable citar al doctor Rincón, quien al respecto manifiesta que *“el que no pueda negarse efectos jurídicos a los mensajes de datos no significa que todos los mensajes tengan el mismo valor probatorio, y ni siquiera que tengan alguno”*¹¹, conforme lo anterior, se evidencia de esta manera que mediante la implementación del principio objeto de estudio se está generando que se dé un mayor espectro a aquellos instrumentos que sirven para materializar operaciones que obliguen a las partes de un negocio, sin que necesariamente dichos instrumentos deban ser papel físico o tradicional y firmas manuscritas en los mismos documentos. En cuanto al valor probatorio de los mensajes de datos, cabe mencionar que si este último hace las veces de un

¹⁰ PEREZ, Marco. "El tratamiento legal de la firma electrónica en Colombia y en el derecho uniforme". Revist@ e – Mercatoria Volumen 1, Número 1. Bogotá, 2002.

¹¹ RINCÓN CÁRDENAS, Erick. "Aproximación jurídica a la firma digital y a los prestadores de servicios de certificación digital". Cámara de Comercio de Bogotá. 2008. Pág. 19.

documento tradicional, en virtud de la equivalencia funcional se tendrá que sirve para probar la existencia de tal información.

Así las cosas, es evidente que el equivalente funcional no es algo distinto de un principio mediante el que se da un mayor espectro a aquellos instrumentos que sirven para que el comercio electrónico se lleve a cabo, es decir, se reconoce que el comercio hoy en día no solo se realiza a través de papeles físicos, sino que se autoriza a que otros instrumentos que sirvan y cumplan la misma finalidad que los documentos físicos, como los mensajes de datos puedan llevar a cabo dicha actividad y por lo tanto brindan la seguridad jurídica que busca la ley objeto de estudio.

Conforme lo anterior, es preciso indicar que el artículo 7 de la Ley 527 de 1999, es una disposición que de acuerdo con el profesor Marco Pérez, corresponde y se asimila al artículo 7 de la Ley Modelo de Comercio Electrónico (LMCE) de la CNUDMI, por lo que es claro que el sistema implementado en el ordenamiento legal colombiano es casi una fiel copia del sistema aprobado en los mecanismos internacionales, donde se reafirma que el mensaje de datos es y hace las veces de un documento firmado físicamente. No obstante lo anterior, el mismo autor señala que el artículo 7 de la Ley 527 de 1999, *“expresa todo requisito de firma manuscrita que esté establecido en cualquier norma vigente, se podrá observar válidamente con un método de firma electrónica, que cumpla los siguientes requisitos mínimos:*

- 1. Debe permitir identificar al iniciador de un mensaje de datos.*
- 2. Debe servir para indicar que el contenido cuenta con su aprobación.*
- 3. Debe ser confiable y aprobado para el propósito por el cual el mensaje fue generado o comunicado”.*

De esta manera resulta claro que todo mensaje de datos que cumpla con los requisitos antes descritos, es decir, que sirva para identificar al emisor del mensaje, contar con la aprobación del contenido del mensaje y que sea confiable y aprobado para el propósito por el cual fue generado el mensaje, se entenderá que el mismo hará las veces de cualquier

documento físico que sea firmado y enviado entre las partes y de esta manera gozará con los mismos efectos probatorios que cualquier otro instrumento.

Por su parte, el profesor Erick Rincón Cárdenas en su obra *“Aproximación Jurídica a la Firma Digital”*, nos ilustra mencionando que *“la función jurídica que cumple la instrumentación escrita y autógrafa respecto a todo acto jurídico, o su expresión oral, la cumple de igual forma la instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, extensión, alcance y finalidad del acto así instrumentado”*¹², esclareciendo así la concepción que se tiene sobre el principio de equivalente funcional, toda vez que la ley es clara en señalar que cualquier documento o mensaje de datos cumple las mismas veces que cualquier documento tradicional.

Así las cosas, es indispensable conocer el artículo 6 de la referida ley ya que el mismo hace alusión al escrito, señalando que en el evento en que se *“requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que este contiene es accesible para su posterior consulta”*; disposición que evidencia y corrobora que la Ley permite que cualquier mensaje de datos haga las veces de documentación escrita y tradicional, permitiendo así que sean utilizados otros instrumentos fuera de los manuscritos para cumplir con la veracidad de la firma plasmada en ellos, de esta manera se debe entender que el principio de equivalente funcional faculta a las partes para hacer uso de mensajes de datos que cumplan con los requisitos del artículo 7 de la Ley 527 para ejercer el comercio, de esta manera la Ley objeto de estudio es clara en otorgar efectos de validez y probatorios a un documento que cumpla con tales lineamientos y/o condicionamientos previstos en la misma.

Adicional a lo anterior, se debe tener en cuenta que el principio de equivalente funcional no solo debe ser observado desde la óptica del escrito, sino que debe tenerse en cuenta desde el punto de vista de la firma, el original y archivo del respectivo documento o mensaje de datos, lo anterior de conformidad con lo dispuesto en los artículos 7, 8 y 9 de la Ley 527 de 1999, que sin lugar a dudas son el pilar fundamental del principio de equivalencia

¹² Ibidem. Pág. 16.

funcional, dado que al hacer una lectura de los mismos, se entiende que el legislador propendió por dar efectos jurídicos a tales instrumentos, y de esta manera agilizar y adecuar las relaciones comerciales a la realidad informática de la época, toda vez que el sistema legal no puede verse obsoleto a tales necesidades.

Conforme a lo anterior, es importante hacer énfasis en que si hay una exigencia consistente en que la información deba constar por escrito, que sea original, que deba estar firmada y de fácil acceso, deberán cumplirse las siguientes condiciones: *“(i) en relación con el escrito, si la información que el mensaje de datos contiene es accesible para su posterior consulta; (ii) en relación con la firma, si se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y que permita indicar que el contenido cuenta con su aprobación y, que el método sea confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado; (iii) en relación con el original, si existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de dato o en alguna otra forma y, de requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se debe presentar(...)”*¹³. Una vez reunidos tales requisitos, podemos encontrar que cualquier mensaje de datos u otro instrumento que cumpla con esos condicionamientos debe ser perfectamente viable y válido ante la legislación colombiana, toda vez que el principio de equivalente funcional será aplicable al caso en concreto ya que dicho instrumento hará las mismas veces que cualquier otro documento que conste por escrito.

Ahora bien, la concepción de equivalente funcional va de la mano con el dinamismo que el mercado informático ha venido implementando en el mercado mundial, por lo que este concepto permite que la legislación no se vea rezagada con respecto a tales novedades, es decir, es un concepto dinámico que se adecuaría a cualquier exigencia y/o mecanismo por medio del que se desarrollen las relaciones contractuales y comerciales de la época, para el efecto el profesor Erick Rincón Cárdenas, anteriormente citado, aterriza la concepción que se tiene sobre el criterio que la Ley 527 tiene sobre el principio de la equivalencia funcional

¹³ Ibidem. Pág. 17.

contenido en los artículos 6, 7, 8 y 9 conllevando necesariamente a que se indique que es *“un criterio flexible que en general tendrá que ser adaptado a los diversos cambios tecnológicos, lo cual se encuentra garantizado por la textura de las normas y la generalidad de referencias que utiliza nuestro legislador. La norma no cierra las posibilidades de sistemas informáticos más avanzados a aquellos que existan en el momento de su promulgación”*¹⁴, concepto que sin lugar a dudas conlleva a que necesariamente nos encontremos en un espacio donde la tecnología ha venido en constante desarrollo y la humanidad se encuentra en la obligación de dar uso de la misma de la manera que más beneficie las relaciones entre los ciudadanos, por tal motivo, se da la posibilidad a que no solo estemos atados a un único mecanismo por el cual se puedan firmar y realizar los negocios jurídicos hoy en día, sino que a medida que la tecnología e industria fueran avanzando, tales instrumentos sirvan para cumplir las veces de cualquier documento físico que conste por escrito, siempre y cuando dicho instrumento cumpla con las condiciones establecidas en la ley y particularmente descritas en el inciso inmediatamente anterior. Ahora bien, no obstante la versatilidad plasmada en el artículo 7 de la Ley 527 de 1999 que permite hacer admisible cualquier mecanismo de firma electrónica, cuando dicha Ley entra a regular de manera concreta la firma digital y le atribuye ciertos efectos particulares, sobre todo en materia de autenticidad, ha dificultado que en la práctica jurídica colombiana se puedan implementar otros mecanismos de firma electrónica, como veremos en detalle en los próximos capítulos.

Continuando con la explicación del equivalente funcional, tal como se mencionó líneas arriba, dicho principio debe ser analizado desde cuatro ópticas que se encuentran debidamente fijadas en la Ley 527 de 1999 en su artículo 6 y siguientes, por lo que pasaremos a explicar brevemente cada uno de ellos así:

a. Equivalente funcional de escrito.

En primera media, es importante tener en cuenta que el equivalente funcional de escrito hace referencia a una aseveración que trae el legislador donde se indica que se permite la

¹⁴ Ibidem. Pág. 18

utilización de mensajes de datos para la acreditación de cualquier tipo de información que deba constar por escrito, es decir, que en el evento de requerir información escrita, no solo tendrá validez aquella que conste en un documento físico común y corriente, sino que la propia ley otorga facultades a que un mensaje de datos tenga los mismos efectos de aquel, por tal motivo es pertinente citar el artículo 6 de la Ley 527, toda vez que la misma disposición consagra dicho requisito que debe contener todo mensaje de datos, así:

“ARTICULO 6o. ESCRITO. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.”

Conforme lo consagrado por dicha disposición, es menester manifestar que todo documento o mensaje de datos contiene información, la cual debe ser plasmada por escrito, es así como lo señala el profesor Erick Rincón Cárdenas cuando nos menciona que *“el legislador consideró que la función primordial que cumple un escrito es la de permitir el acceso de la información consignada en el mismo en forma posterior a la creación del mensaje. Los mensajes de datos, por tanto, deben cumplir con esa función para ser considerados escritos”*¹⁵. Resulta evidente entonces que cualquier mensaje de datos o documento debe contener la información de manera escrita, ya que es el mecanismo mediante el cual se permite la consulta del mismo con posterioridad a la creación de tal documento, resultando necesario que los usuarios de estos instrumentos deban plasmar la manifestación de su voluntad en escritos, de esta manera lo que se pretende es su posterior consulta con la finalidad de observar lo dispuesto por el usuario, es decir, corroborar la información que se plasmó en tal instrumento de manera originaria sin que esa información haya sido objeto de modificación alguna.

b. Equivalente funcional de firma.

¹⁵ Ibidem. Pág. 20.

Es importante conocer el significado del concepto de firma, para lo que nos permitimos referirnos al Diccionario de la lengua española de la Real Academia que nos indica que la firma es *“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”*¹⁶; concepto del que se deriva claramente que la firma es aquel reconocimiento que da una persona a un documento, es decir, con la firma se aprueba el documento mismo y lo que este contenga, viene a ser entonces la manifestación de voluntad con la que se reconoce la autoría y contenido del respectivo documento.

De esta manera, se pasa a abordar el concepto de equivalencia funcional de firma que es aquel atributo que la propia ley otorga a aquellos mensajes de datos que cumplan con los requisitos consagrados en el artículo 7 de la pluricitada ley, esto es que el mensaje de datos permita la identificación fiable del originador del mismo sin que haya posibilidad de alterar el mismo y del que se acredite que el originador del mensaje creó o aprobó el mismo para así haberlo enviado, de esta manera, es claro que hay una concesión a otorgar aquellos efectos jurídicos y probatorios a los mensajes de datos de los que no quede duda alguna del originador del mismo, esto es, que siempre y en todo momento se pueda observar el mensaje de datos original donde se evidencie la aprobación por parte de su creador; de esta manera se brinda una certeza y confianza en los usuarios de tales mecanismos, donde pueden confiar en que la manifestación de la voluntad es veráz y proveniente de su originador.

Así las cosas, la ley objeto de estudio permite la utilización de firmas electrónicas o plasmadas en medios electrónicos para la realización de cualquier negocio jurídico, siempre que tal instrumento cumpla con los requerimientos de la disposición arriba indicada, es así como el legislador ha permitido la utilización de estos sistemas para dar la agilidad necesaria a los negocios de una manera segura y eficaz, evitando de esta manera que se obligue a los contratantes a plasmar su firma en un documento tradicional que conste en medios físicos.

¹⁶ Fuente de internet. <http://lema.rae.es/drae/?val=firma>

Teniendo en cuenta lo anterior, pasamos a citar el artículo 7 de la Ley 527 de 1999, que consagra la firma que deben contener los mensajes de datos para que los mismos se entiendan han sido suscritos por una persona, así:

“ARTICULO 7o. FIRMA. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

- a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;*
- b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.*

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma”.

Conforme la anterior disposición y la definición del concepto de firma, es menester hacer mención a que todo documento una vez sea firmado por una persona, el mismo gozaría de toda validez y reconocimiento por parte del originador, por lo que inmediatamente le será aplicable lo contenido en el mismo, es decir, será vinculante para esta parte. “La Ley Modelo de Comercio Electrónico LMCE indicó las siguientes funciones generales de una firma: a) Identificar a una persona. b) Dar certeza a la participación directa de esa persona en el acto de firmar. c) Asesorar a esa persona con el contenido de un documento.”¹⁷, funciones que ampliamente están en concordancia con la definición de una firma, toda vez que es el reconocimiento y vínculo que hay entre una persona y un documento que ha reconocido como propio.

En este mismo orden de ideas, el profesor Erick Rincón Cárdenas señala que el artículo 7 de la referida ley dispone que la firma tiene la finalidad de *“a) Identificar al iniciador de*

¹⁷ RINCÓN CÁRDENAS, Erick. “Aproximación jurídica a la firma digital y a los prestadores de servicios de certificación digital”. Cámara de Comercio de Bogotá. 2008. Pág. 22.

un mensaje de datos. b) Vincular al iniciador con el contenido del documento firmado”¹⁸, requisitos que están en total acuerdo con lo que se entiende como firma, ya que en efecto la firma de un mensaje de datos debe identificar a la persona que suscribe tal instrumento y de igual manera lo vincula con el mismo, esto es, hace que el documento sea propio y no lo pueda desconocer.

En igual sentido, el literal b de tal disposición –artículo 7- dispuso una limitación al uso de los dispositivos electrónicos, ya que se indica que el método debe ser tanto confiable como apropiado para los fines en los que ha sido previsto el mensaje, por lo que al cumplir con este par de requisitos, en efecto el mensaje de datos hará las veces de un firma común y corriente, es decir, tendrá la misma validez que cualquier documento tradicional, ello de conformidad con la equivalencia funcional, al respecto el Doctor Rincón señaló *“si un documento electrónico está o no firmado depende de dos grandes factores: el método de firma utilizado y el tipo de mensaje de datos que se está firmando. El solo hecho de usar un dispositivo de firma como los mencionados anteriormente no es suficiente para considerar que el documento se encuentra firmado, sino que el método debe cumplir con dos requisitos valorativos: **debe ser confiable y debe ser apropiado**”¹⁹*. De esta manera se explica que la firma debe contar con una serie de dispositivos de seguridad con la finalidad que el mensaje no sea objeto de manipulación o alteración alguna, conllevando necesariamente a que sea confiable para los actores lo que permitirá sin lugar a dudas el desarrollo de los negocios por este medio.

En este orden de ideas, las entidades de certificación que serán estudiadas próximamente, tienen el deber de garantizar que se cumpla esta equivalencia funcional respecto al escrito, toda vez que el legislador ha transferido tal responsabilidad a este tipo de entidades, lo que conlleva necesariamente a que se garantice la confidencialidad, integridad y la autenticidad de aquellas firmas digitales que sean transadas a través de estas entidades; ahora bien, es claro que la firma digital fuera de ser utilizada por medio de las entidades de certificación, debe cumplir con los parámetros arriba señalados, toda vez que la ley permite su utilización

¹⁸ Ibidem. Pág. 22.

¹⁹ Ibidem. Pág. 24.

y brinda la validez del caso, siempre que tal firma digital no sea utilizada para la comisión de infracciones, por tal motivo, se otorga esta responsabilidad a terceras partes como las entidades de certificación, “la ley colombiana que regula el comercio electrónico, en la parte técnica sobre firma digital y entidades prestadoras de servicios de certificación establece condiciones adicionales de seguridad técnica jurídica a las transacciones electrónicas, que garantizan confidencialidad, integridad, identificación o autenticación y no rechazo(...) **la confidencialidad** garantiza que los mensajes de datos lleguen, exclusivamente, a las personas autorizadas para ello; con **la integridad**, que el mensaje de datos no sea interceptado y modificado durante el envío; con **la autenticación**, y mediante el uso de la firma digital, que se reconozca al titular de la firma y del mensaje, y, con el no rechazo y a través del uso de los servicios de certificación digital, se podrá tener claridad de que el destinatario de un mensaje no desconocerá su recepción y que el autor no negará su autoría”²⁰, parámetros que sirven de fundamento para determinar la seguridad que debe contener una firma y permita que la misma haga las veces que cualquier firma que sea plasmada en un documento en papel.

c. Equivalente funcional de original.

La originalidad es otro pilar fundamental de la equivalencia funcional, donde se evidencia que todo mensaje de datos hará las veces de un documento firmado en papel, de esta manera, es claro que todo mensaje de datos debe cumplir con la originalidad, es decir, que siempre y en todo momento se pueda tener el documento original que inicialmente fue originado, garantizando así que dicho documento no ha sido alterado por el originador del mismo o por un tercero; es entonces la originalidad parte fundamental de la equivalencia funcional, toda vez que al otorgar la validez a todo mensaje de datos, este deberá cumplir con este requisito ya que es importante brindar tal seguridad a las partes que empiecen a utilizar la firma digital para agilizar los negocios jurídicos a celebrar, por lo tanto todo mensaje de datos debe cumplir con lo estipulado en el artículo 8 de la Ley 527 de 1999, que reza:

²⁰ Ibidem. Pág. 25 y ss.

“ARTICULO 8o. ORIGINAL. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

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

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original”.

Conforme a lo señalado en esta disposición, es claro que en el evento en que la información que reposa sobre un mensaje de datos deba ser presentada y conservada en su forma original, se debe garantizar la genuinidad e integridad del mismo, esto es que el mensaje de datos -o cualquier otro instrumento que haga estas veces- pueda ser conservado en su integridad. En este orden de ideas, *“se entiende satisfecho el requisito de original siempre que exista una garantía confiable de que la información se ha conservado íntegra desde el momento en que por primera vez se generó en su forma definitiva. Esto quiere decir que, en principio, cualquiera de las copias realizadas de un documento cualquiera podría ser considerado un original para efectos probatorios. Resultaría indiferente establecer cuántas copias se han realizado, o si el archivo electrónico que se examina es una copia de una copia o una copia del primer archivo que se creó”*²¹, de esta manera la norma es clara en exigir que lo que se requiere es garantizar de manera confiable que la información se conservó desde que se creó, por lo que resulta importante guardar una copia fiel del original o en su defecto no alterarlo, ello con la finalidad de brindar aquella seguridad jurídica que exige la utilización de los mensajes de datos, por su parte, se requiere que estos documentos electrónicos se puedan mantener archivados de manera fidedigna u original para su

²¹ Ibidem. Pág. 29.

posterior consulta, brindando así una confianza en estos mecanismos que no son los comúnmente utilizados.

Así las cosas, a modo de ejemplo vale la pena mencionar algunos mecanismos para mantener la originalidad de un documento sin que esto conlleve a la afectación o alteración del mensaje de datos.

- El profesor Rincón ha mencionado la necesidad de tener un sistema ampliamente seguro, por medio de la implementación de dos claves; la primera de ellas es pública y la segunda es privada, estas dos claves permiten que cualquier usuario pueda conocer el documento objeto de firma, sin embargo para tener certeza del origen de la firma del mismo, se tiene una clave privada que solo es digitada por el firmante. De esta manera se permite que una parte pueda acceder al documento una vez lo haya firmado la otra mediante el ingreso de estos códigos.

Este tipo de registro de claves se tramitará y estará bajo custodia de cada una de las partes.

- La Ley 527 de 1999 dispuso y reglamentó parcialmente unas entidades de certificación, las cuales tienen como finalidad el almacenamiento de registros, claves, documentos, entre otros, lo cual brinda la seguridad a todos y cada uno de los usuarios de la firma digital en cualquier documento o mensaje de datos, ya que al ser ajenos al negocio jurídico a celebrar guardan fidedignamente la información registrada. Particularmente estas entidades de certificación serán ahondadas con mayor precisión en los capítulos siguientes.

d. Equivalente funcional de archivo y conservación.

El último de los elementos que tiene relevancia con respecto al equivalente funcional es el referente a la conservación y archivo de los mensajes de datos, que tal como en los anteriores subcapítulos se ha venido explicando, toda firma digital plasmada en un mensaje

de datos debe poder archivar y consultarse como originalmente fue emitida, lo anterior con la finalidad de brindar la seguridad requerida por los usuarios, de tal forma, la Ley 527 de 1999 dispuso en su artículo 12 lo siguiente:

“ARTICULO 12. CONSERVACION DE LOS MENSAJES DE DATOS Y DOCUMENTOS. Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

- 1. Que la información que contengan sea accesible para su posterior consulta.*
- 2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y*
- 3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.*

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta”.

Conforme tal disposición, se evidencia que lo que pretende la ley es que en el comercio electrónico, todo mensaje de datos pueda ser consultado con posterioridad a la emisión del mismo siempre que este obedezca al que originalmente se emitió y que se permita conocer el origen y destino del mensaje así como la fecha, hora, entre otros aspectos del mensaje, lo que permite ineludiblemente tener certeza que se trata del mismo documento o mensaje de datos sin que el mismo sea susceptible de ser alterado.

De esta manera, se concluye que el principio de equivalente funcional debe reunir los cuatro elementos anteriormente señalados, particularmente refiriéndonos a que todo mensaje de datos o cualquier instrumento que haga las veces de un documento por escrito en papel y que se encuentre debidamente firmado, ya que se debe blindar a los mensajes de

datos para que gocen de amplia validez jurídica y tengan valor probatorio en un eventual proceso o se presente cualquier duda respecto del mensaje de datos en el que conste la manifestación de la voluntad de una de las partes. No obstante lo anterior, en el evento en que el mensaje de datos no cumpla con los elementos antes mencionados, puede decirse que el instrumento no sirve para los fines previamente indicados en la ley, lo que resulta aplicable a cualquier mecanismo que sea equivalente al mensaje de datos, esto es el equivalente funcional.

Por último y para concluir el asunto de equivalente funcional, debemos mencionar que este principio constituye un mecanismo mediante el cual las personas pueden utilizar instrumentos fuera de los manuscritos, tales como los mensajes de datos con la finalidad de realizar las operaciones comerciales con la agilidad que sea necesaria sin la necesidad de transferir o cruzar documentos en papel para llevar a cabo las mismas, al efecto el Consejo de Estado mediante sentencia del 18 de marzo de 2010 bajo radicado 1989, dispuso en su parte motiva que *“los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la ley”*²², lo anterior de conformidad con la exposición de motivos de la Ley 527 de 1999, cita que permite tener presente que el equivalente funcional se da sobre cualquier instrumento que haga las veces de cualquier documento en papel firmado por las partes, tal como lo es el mensaje de datos.

²² CONSEJO DE ESTADO, Sala de Consulta y Servicio Civil. Rad. 1989 Sentencia del 18 de marzo de 2010. Consejero Ponente. Enrique José Arboleda Perdomo.

III. EL CÓDIGO GENERAL DEL PROCESO Y LA PRESUNCIÓN DE AUTENTICIDAD DE LOS MENSAJES DE DATOS: MODIFICACIÓN A LA LEY DE COMERCIO ELECTRÓNICO.

Con la expedición de la Ley 1564 de 2012 – Código General del Proceso – el legislador introdujo una serie de modificaciones particulares en materia probatoria, y una de dichas modificaciones consiste en atribuirle expresamente a los mensajes de datos la calidad de documento y en dotarlos de presunción de autenticidad. Estas nuevas cualidades que han sido atribuidas a los mensajes de datos, buscan dotarlos de plena eficacia probatoria en el curso de todas las actuaciones judiciales y extrajudiciales, en las cuales resulte aplicable dicho Código.

A través del presente capítulo pretendemos poner de presente la importancia de estas disposiciones desarrolladas por el Código General del Proceso, mediante las cuales se subsanan graves falencias contenidas en la Ley de Comercio Electrónico – Ley 527 de 1999 – y sus decretos reglamentarios, que implicaban que la misma fuera retrograda frente a las necesidades del comercio electrónico en particular frente a la utilización de diversas categorías de firmas electrónicas, y los rigurosos requisitos exigidos por la Ley 527 - antes de sus recientes modificaciones - para acreditar la autenticidad de dichas firmas electrónicas.

3.1. Noción de mensaje de datos desarrollada por la Ley 527 de 1999.

Previo a entrar a profundizar en la problemática que presentaba la Ley de Comercio Electrónico frente a la autenticidad de los mensajes de datos, veamos qué define la legislación colombiana como mensaje de datos.

El literal a) del artículo 2 de la Ley 527 de 1999 define los mensajes de datos como:

“ (...)La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;”

Como puede observarse, la definición de mensaje de datos es muy amplia al incluir verbos rectores como enviar, recibir, almacenar y comunicar, que implican que pueda considerarse como mensaje de datos un sinnúmero de información a través de medios electrónicos.

Veamos el alcance dado por la jurisprudencia de la Corte Constitucional a esta noción de mensaje de datos incluida en la Ley de Comercio Electrónico:

“El mensaje electrónico de datos, se considera la piedra angular de las transacciones comerciales telemáticas.

Por ello la ley lo describe en la siguiente forma:

***"Mensaje de datos:** la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax". (Artículo 2º literal b).*

La noción de "mensaje" comprende la información obtenida por medios análogos en el ámbito de las técnicas de comunicación modernas, bajo la configuración de los progresos técnicos que tengan contenido jurídico.

Cuando en la definición de mensaje de datos, se menciona los "medios similares", se busca establecer el hecho de que la norma no está exclusivamente destinada a conducir las prácticas modernas de comunicación, sino que pretenden ser útil para involucrar todos los adelantos tecnológicos que se generen en un futuro.

El mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento.”²³

No cabe la menor duda que el tráfico jurídico actual evidencia una infinidad de actos, manifestaciones de voluntad o contratos que se materializan por medio de mensajes de datos, de ahí la importancia de otorgarle a los mismos plena eficacia probatoria como si se tratara de actuaciones manuscritas. Es en este sentido, que la Corte Constitucional

²³ Cfr. CORTE CONSTITUCIONAL, sentencia C – 622 de 2000 M.P. Fabio Morón Díaz y sentencia C – 831 de 2001. M.P. Álvaro Tafur Galvis.

reconociendo la necesidad de mantener la legislación en materia de comercio electrónico acorde con el dinamismo de las transacciones realizadas a través de mensajes de datos, destaca la inclusión de la expresión “medios similares” dentro de la definición de mensaje de datos dada por nuestra legislación. Dicha inclusión permite mantener la definición de mensaje de datos vigente frente a todos los adelantos tecnológicos que se generen en el futuro, sin restringirse a los medios o tecnologías descritos en la norma, lo cual sin duda redundará en la eficacia probatoria que tendrá el desarrollo de nuevas tecnologías, que gracias a la amplitud de la definición podrán ser consideradas como mensajes de datos y en consecuencia podrán gozar de los efectos jurídicos que la legislación colombiana le atribuye a los mismos, siendo el más importante de ellos la presunción de autenticidad de la cual hablaremos en este capítulo.

Ahora bien, teniendo claro la definición que nuestra legislación adopta de mensaje de datos, definición idéntica a la desarrollada por el artículo 2 de la Ley Modelo de Comercio Electrónico de 1996 desarrollada por la CNUDMI, procederemos a profundizar en aquellos aspectos problemáticos de la Ley de Comercio Electrónico en materia de autenticidad de mensajes de datos y que gracias al Código General del Proceso vienen a ser solucionados.

3.2. Problemática de la Ley de Comercio Electrónico frente a los mensajes de datos: regulación excesiva y tratamiento preferencial de la firma digital.

La Ley 527 de 1999 reproduce casi en su totalidad la Ley Modelo de Comercio Electrónico de 1996 desarrollada por la CNUDMI, pero como es costumbre en las adaptaciones que en muchos casos nuestros legisladores hacen de disposiciones normativas internacionales para incorporarlas al ordenamiento jurídico interno, se peca de exceso de regulación o se hacen variaciones que terminan por modificar por completo el espíritu de la normatividad que se está implementando

En efecto, como ya lo veníamos anticipando la mayor dificultad que entrañan las relaciones jurídicas a través de mensajes de datos está en acreditar la autenticidad de dicho mensaje, autenticidad que se verifica a través del mecanismo de firma electrónica utilizado y que

dicho mecanismo satisfaga los presupuestos establecidos por el artículo 7 de la Ley 527 de 1999. El profesor Marco Pérez²⁴ nos pone de presente esta problemática, veamos:

*“Las denominadas firmas electrónicas, poseen elementos que no son los mismos de la noción tradicional de firma, porque en un entorno electrónico, entre otras circunstancias, el original de un documento no se puede distinguir de una copia, ni lleva una firma manuscrita y no reposa sobre un papel.”*²⁵

Esta dificultad en torno a la autenticidad que implican las transacciones a través de medios electrónicos pretende ser superada mediante la incorporación de mecanismos de firma electrónica que cumplan con los requisitos señalados en el artículo 7 de la Ley 527 de 1999, que desarrolla el principio de “equivalencia funcional” de la firma tal como pudo apreciarse en detalle en el capítulo precedente de este trabajo. Los requisitos que señala el artículo 7 son: (i) método que permita identificar al iniciador del mensaje de datos, (ii) método que permita identificar que el contenido del mensaje de datos cuenta con la aprobación del iniciador y (iii) que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

De los anteriores requisitos aquel que en la práctica mayor relevancia probatoria implica es el consistente en un *método que permita identificar que el contenido del mensaje de datos cuenta con la aprobación del iniciador*, en otras palabras acreditar la autenticidad y veracidad del documento electrónico.

La Sala de Casación Civil de la Corte Suprema de Justicia ha destacado la importancia de estos atributos de la prueba documental para determinar su eficacia probatoria:

“Es incontestable, subsecuentemente, que la autenticidad y la veracidad son atributos distintos de la prueba documental, pues, como ha quedado dicho, el primero tiene que ver con la plena identificación del creador del documento, con miras a “establecer la pertenencia del documento a la persona a quien se atribuye, es decir, la correspondencia del sujeto que aparece elaborándolo o firmándolo, con

²⁴ Investigador de la Universidad Externado de Colombia.

²⁵ PEREZ, Marco. "El tratamiento legal de la firma electrónica en Colombia y en el derecho uniforme". Página 3. Revist@ e – Mercatoria Volumen 1, Número 1. 2002.

la persona que realmente lo hizo” (sent. 20 de octubre de 2005, exp. 1996 1540 01), mientras que la veracidad concierne con el contenido del documento y la correspondencia de éste con la realidad o, en otros términos, está referida a la verdad del pensamiento ,declaración o representación allí expresados.”²⁶

Ahora bien, teniendo claro que el aludido requisito del artículo 7 hace referencia a la autenticidad y veracidad del documento electrónico, ¿en la práctica como logran probarse dichos atributos? Como veremos en los párrafos siguientes, dicho requisito se acredita mediante un certificado digital, tratándose de firma digital, bajo el esquema original de la Ley 527 de 1999, o mediante un certificado de firma electrónica, con base en las modificaciones realizadas a la Ley 527 de 1999.

A pesar de que el artículo 7 consagra un principio general que hace admisible cualquier mecanismo de firma electrónica que satisfaga los requisitos anteriormente mencionados, lo cierto es que la Ley 527 y sus Decretos reglamentarios mandan al traste con ese principio general cuando entran a regular de manera concreta la firma digital – especie de firma electrónica – dotándola de un carácter preferencial frente a otros métodos de firma electrónica y generando que durante todo el tiempo de vigencia que ha tenido la Ley de Comercio Electrónico el único mecanismo que en la práctica es utilizado y admisible sea el de la firma digital, la cual se ha tornado compleja y arcaica frente a otros mecanismos de firma electrónica y frente a las realidades del comercio electrónico, como expondremos a continuación:

La Ley Modelo de Comercio Electrónico de la CNUDMI no regula la firma digital, toda vez que como Ley Modelo establece principios generales y orientadores, no obstante lo anterior cuando nuestro legislador inspirado en dicha Ley Modelo profiere la Ley 527 de 1999 define y regula de manera concreta la firma digital, regulación que sobraba, toda vez que el artículo 7 era un criterio orientador suficientemente claro para toda clase de firmas electrónicas, toda vez que se limitaba a señalar los requisitos o criterios necesarios para brindar de eficacia probatoria y equivalencia funcional a cualquier mecanismos de firma electrónica sin distinción.

²⁶ Cfr. CORTE SUPREMA DE JUSTICIA, Sala de Casación Civil. Sentencia del 20 de octubre de 2005 y sentencia del 16 de diciembre de 2010. M.P. Pedro Octavio Munar Cadena.

A continuación, procederemos a exponer las principales complejidades que implica la regulación dada en nuestro ordenamiento jurídico a la firma digital y por qué la utilización de la misma ha restringido la implementación de otros métodos más efectivos y sencillos.

El literal c) del artículo 2 de la Ley 527 de 1999 define la firma digital como:

“(…) un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;”

Posteriormente, el artículo 28 consagra los efectos jurídicos y atributos de la firma digital. Veamos:

“ARTICULO 28. ATRIBUTOS JURIDICOS DE UNA FIRMA DIGITAL. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

PARAGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

- 1. Es única a la persona que la usa.*
- 2. Es susceptible de ser verificada.*
- 3. Está bajo el control exclusivo de la persona que la usa.*
- 4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.*
- 5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.”*

Como puede observarse, el citado artículo 28 consagra una presunción de autenticidad de la firma digital, equiparándola a la firma manuscrita, presunción que solo será aplicable con el cumplimiento de una serie de requisitos muy engorrosos, que en la práctica solamente vienen a acreditarse mediante un certificado digital expedido por una entidad de

certificación autorizada por la Superintendencia de Industria y Comercio. Dicho requisito de certificación es establecido por el artículo 15 del Decreto 1747 de 2000 que reglamenta el artículo 28 de la Ley 527 de 1999. Vale la pena destacar que estos requisitos deben cumplirse de manera concurrente para que pueda aplicarse la presunción. Veamos qué nos dice el profesor Jairo Parra Quijano sobre la forma de acreditar judicialmente el cumplimiento de los requisitos consagrados en el parágrafo del artículo 28:

“Es importante precisar que si la información que se pretende hacer valer judicialmente consta en un mensaje de datos firmado digitalmente y dicha firma se respalda en un certificado digital, no se requiere que el interesado, pruebe la presencia de los atributos del parágrafo del artículo 28, basta con que allegue con la demanda, el mensaje de datos firmado, el certificado digital vigente, la resolución emitida por la Superintendencia de Industria y Comercio, que autoriza las actividades de la entidad de certificación que emitió el certificado y el contrato entre la entidad de certificación y el suscriptor que acredite expresamente los usos para los cuáles se podía utilizar el certificado.”²⁷

De la relación de requisitos que nos pone de presente el profesor Jairo Parra, puede apreciarse lo tortuoso que es bajo el esquema de la Ley 527 de 1999 en concordancia con el Decreto reglamentario 1747 de 2000, demostrar judicialmente la autenticidad de una firma digital. El solo hecho de tener que contar con certificados para probar dicha autenticidad, es un requisito que atenta contra la dinámica de las relaciones contractuales a través de medios electrónicos.

Ahora bien, si no se cuenta con el certificado digital, ¿cómo se prueban los requisitos exigidos por el parágrafo del artículo 28 de la Ley 527 de 1999?:

“La inquietud que surge, es si las firmas digitales que no cuenten con el respaldo de un certificado digital se entenderán como no validas a la luz del artículo en mención.

²⁷ QUIJANO PARRA, Jairo. “Manual de derecho probatorio.” Ediciones Librería Profesional, Bogotá, 2002. Página 481.

Si la firma digital del mensaje de datos no cuenta con el respaldo de un certificado digital, el interesado debe probar la presencia de los atributos del artículo 28, para que dicha firma se entienda equivalente a una firma manuscrita. Los artículos 7 y 28 de la Ley 527 de 1999, que definen firma y firma digital además de ser imperativos, sirven de orientación cuando el derecho interno deje totalmente a discreción de las partes la autenticación de los mensajes de datos.”²⁸

Como puede observarse de lo expuesto en los párrafos precedentes, la Ley de Comercio Electrónico solamente dota de presunción de autenticidad una sola categoría de firma electrónica – la firma digital – dejando por fuera otros mecanismo de firma, autenticidad que se presumirá mediante la presentación de un certificado digital o en su defecto mediante la dispendiosa tarea de acreditar todos y cada uno de los requisitos establecidos por el artículo 28 de la Ley 527 de 1999.

En idéntico sentido, la jurisprudencia de la Sala de Casación Civil de la Corte Suprema de Justicia ha señalado que solo mediante la firma digital un documento electrónico estará provisto de presunción de autenticidad:

“Dicha especie de firma electrónica se equipara a la firma ológrafa, por cuanto cumple idénticas funciones que ésta, con las más exigentes garantías técnicas de seguridad, pues no sólo se genera por medios que están bajo el exclusivo control del firmante, sino que puede estar avalada por un certificado digital reconocido, mecanismos que permiten identificar al firmante, detectar cualquier modificación del mensaje y mantener la confidencialidad de éste.

De manera, pues, que el documento electrónico estará cobijado por la presunción de autenticidad cuando hubiese sido firmado digitalmente, puesto que, al tenor de lo dispuesto en el artículo 28 ibídem, se presumirá que su suscriptor tenía la intención

²⁸ PEREZ, Marco. "El tratamiento legal de la firma electrónica en Colombia y en el derecho uniforme". Página 11. Revist@ e – Mercatoria Volumen 1, Número 1. Bogotá, 2002.

de acreditarlo y de ser vinculado con su contenido, claro está, siempre que ella incorpore los siguientes atributos: a) fuere única a la persona que la usa y estuviere bajo su control exclusivo; b) fuere susceptible de ser verificada; c) estuviere ligada al mensaje, de tal forma que si éste es cambiado queda invalidada; y d) estar conforme a las reglamentaciones adoptadas por el Gobierno Nacional. Por lo demás, será necesario que hubiese sido refrendada por una entidad acreditada, toda vez, que conforme lo asentó la Corte Constitucional, éstas “certifican técnicamente que un mensaje de datos cumple con los elementos esenciales para considerarlo como tal, a saber la confidencialidad, la autenticidad, la integridad y la no repudiación de la información, lo que, en últimas permite inequívocamente tenerlo como auténtico” (C-662 de 2000), pues, a decir verdad, ellas cumplen una función similar a la fedante.”²⁹(Subrayado como énfasis)

Adicionalmente a lo anterior, la Ley de Comercio Electrónico solamente le atribuía a las entidades de certificación la facultad de certificar firmas digitales – artículo 30 -, facultad que vino a ser ampliada por el Decreto 019 de 2012 a todas las firmas electrónicas, como veremos en capítulos posteriores. Esta restricción ponía en desventaja a otros mecanismos de firma electrónica, toda vez que la demostración de la confiabilidad de los mismos era mucho más compleja que la de la firma digital, para la cual bastaba la expedición de un certificado digital que avalara su confiabilidad. Además como veremos a continuación, la firma digital ya ha entrado en desuso dado a que existen mecanismos de firma electrónica más fiables, efectivos y prácticos que van en armonía con el dinamismo del comercio electrónico.

La firma digital es un método de firma electrónica basado en “*algoritmos de encriptación asimétrica y que utilizan llaves o claves públicas y privadas en el proceso de creación y verificación de las firmas. Esta tecnología de firma, también se denomina criptografía de clave pública.*”³⁰

²⁹ CORTE SUPREMA DE JUSTICIA, Sala de Casación Civil, sentencia del 16 de diciembre de 2010. M.P. Pedro Octavio Munar Cadena.

³⁰ MENDÍVIL, Ignacio. “ABC de los documentos electrónicos seguros”. Página 3. México, 1999.

Así las cosas, la firma digital se caracteriza por tener un sistema de *passwords* o contraseñas, el cual implica riesgos de extravío, exposición pública o fraude que atentan en contra de la seguridad de dicho mecanismo.

En consideración a los anteriores riesgos, han surgido mecanismos de firma electrónica como aquellos basados en autenticación biométrica que implican una mayor fiabilidad, practicidad y seguridad:

“Estos métodos de autenticación biométrica han desplazado el uso de passwords y claves personales, para proteger el acceso a las redes de las empresas y a la información digital altamente sensible de las organizaciones; porque los passwords y claves personales son fácilmente expuestos, extraviados o inapropiadamente compartidos. Además no hay necesidad de realizar reposición de tarjetas de acceso perdidas o nueva asignación de contraseñas olvidadas, ya que las características corporales no cambian, no se modifican, extravían, ni se pueden prestar o ceder.”³¹

Los mecanismos de firma electrónica consistentes en autenticación biométrica son conocidos como métodos basados en “algo que usted es”, mientras que los mecanismos consistentes en contraseñas, como la firma digital, son basados en el criterio “algo que usted tiene o posee”.³²

De acuerdo con lo hasta aquí expuesto, podemos observar que hasta la expedición del Código General del Proceso y otra normativa reciente como el llamado Decreto Anti trámites – Decreto 019 de 2012 – y el Decreto 2364 de 2012 que reglamenta el artículo 7 de la Ley 527 de 1999, la única manera práctica de acreditar la autenticidad de un documento electrónico era a través de una firma digital la cual debía ir acompañada de su correspondiente certificado digital.

³¹ PEREZ, Marco. "El tratamiento legal de la firma electrónica en Colombia y en el derecho uniforme". Página 8. Revist@ e – Mercatoria Volumen 1, Número 1. Bogotá, 2002.

³² Cfr. Ibíd. Páginas 7 y 8.

Ahora que tenemos claro la problemática en torno a la firma digital regulada por la Ley de Comercio Electrónico y la complejidad para demostrar la autenticidad de documentos electrónicos mediante otros mecanismos de firma electrónica, veamos cómo el Código General del Proceso termina con ese tratamiento preferencial de la firma digital frente a otros métodos de firma electrónica.

3.3. El Código General del Proceso y la presunción de autenticidad de los mensajes de datos.

En efecto, la solución que trae el Código General del Proceso en su artículo 244 es muy simple: dotar de presunción de autenticidad a todo documento presentado en forma de mensaje de datos, presunción que no está condicionada al cumplimiento de requisitos como ocurre con el parágrafo del artículo 27 de la Ley 527 de 1999.

“ARTÍCULO 244. DOCUMENTO AUTÉNTICO. Es auténtico un documento cuando existe certeza sobre la persona que lo ha elaborado, manuscrito, firmado, o cuando exista certeza respecto de la persona a quien se atribuya el documento.

(...)

La parte que aporte al proceso un documento, en original o en copia, reconoce con ello su autenticidad y no podrá impugnarlo, excepto cuando al presentarlo alegue su falsedad. Los documentos en forma de mensaje de datos se presumen auténticos.

Lo dispuesto en este artículo se aplica en todos los procesos y en todas las jurisdicciones.” (Subrayado como énfasis)

Es importante aclarar que el ámbito de aplicación de esta disposición normativa se circunscribe a las actuaciones judiciales en donde sea aplicable el Código General del Proceso. Así las cosas el artículo 28 de la Ley 527 de 1999 que establecía una serie de requisitos para acreditar la presunción de autenticidad de una firma digital de un documento

electrónico ha quedado tácitamente derogado por el artículo 244 del Código General del Proceso, tratándose de actuaciones judiciales. Lo anterior toda vez que este último es una ley posterior y está regulando de manera especial la materia al hacer referencia expresa a la presunción de autenticidad de los “documentos en forma de mensaje de datos”. En relación a actuaciones no judiciales deberá tenerse en cuenta las modificaciones introducidas por el Decreto 2364 de 2012 y el Decreto 019 de 2012, que serán objeto de estudio en los próximos capítulos.

Las implicaciones probatorias que trae el artículo 244 citado - que como se anotó modifica la Ley 527 de 1999 - son de gran importancia, toda vez que con esta presunción se invierte la carga de la prueba en el sentido de que quien aporta el documento electrónico ya no deberá acreditar su autenticidad, ni demostrar la confiabilidad del mecanismo de firma electrónica como lo dispone el artículo 7 de la Ley 527 de 1999. Ahora corresponderá a la persona contra quien se aporta el documento en forma de mensaje de datos desvirtuar la presunción de autenticidad del mismo.

Sin duda esta norma va a garantizar mayor seguridad, confiabilidad y celeridad en el tráfico de las relaciones jurídicas por medios electrónicos, haciendo que nuestra legislación en comercio electrónico esté acorde a las necesidades de un mundo actual donde la rapidez en las transacciones es un tema de vital importancia para los sujetos en ellas involucradas, así como la certeza de contar con una legislación que protege y da plena eficacia probatoria a los mecanismos de autenticidad que implementen las partes en sus relaciones jurídicas.

De esta manera podemos concluir que el Código General del Proceso modifica la Ley 527 de 1999 y le otorga a toda la información en forma de mensaje de datos plena eficacia probatoria, siendo indiferente el mecanismo de firma electrónica utilizado para brindarle autenticidad al mensaje de datos.

Por último, es importante señalar que de acuerdo con el artículo 627 del Código General del Proceso, la presunción de autenticidad de los mensajes de datos regulada por este código entrará en vigencia a partir del 1 de enero de 2014, hasta esa fecha nos seguiremos rigiendo

por las disposiciones de la Ley 527 de 1999 con las modificaciones realizadas mediante el Decreto Anti trámites y el Decreto 2364 de 2012, de los cuáles hablaremos en los próximos capítulos.

IV. ENTIDADES DE CERTIFICACIÓN.

Teniendo en cuenta la complejidad que trae consigo la implementación de la firma electrónica en nuestro ordenamiento jurídico, toda vez que no ha sido fácil que la misma genere confianza y seguridad en las personas, así como que la gente no sabe cómo poder implementar la misma para la celebración de cualquier tipo de negocio, se han creado las entidades de certificación, precisamente para superar este tipo de inconvenientes.

De esta manera una entidad de certificación es una persona que se encuentra ampliamente facultada por el legislador para emitir certificaciones respecto de las firmas digitales de aquellas personas que se encuentran en ella registradas, por lo que el literal (d), artículo 2 de la Ley 527 de 1999 se ha encargado de definir la entidad de certificación como *“aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales”*

Al respecto el doctor Henao Restrepo señaló que *“Las entidades de certificación son aquellas personas jurídicas y privadas, incluidas las Cámara de Comercio, que poseen hardware y software necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación del archivo de documentos soportados en mensajes de datos”*³³

Así las cosas, tenemos que una entidad de certificación según la Ley 527 de 1999 se basaba únicamente en la prestación de ciertos servicios relacionados con la firma digital, sin embargo sus funciones se detenían ahí, razón por la que con el Decreto 19 de 2012 se amplió su aplicación a las demás clases de firma electrónica, ya sea generándolas o emitiendo certificados sobre estas, de esa manera se da un mayor espectro a las personas para la utilización de estos nuevos mecanismos, esta regulación permite que las entidades de certificación no solo se basen en el registro de ciertas firmas, sino que adicionalmente

³³ HENAO RESTREPO, Darío. *“Ley de Comercio Electrónico en Colombia (ley 527 de 1999)”* en Nuevos Retos del Derecho Comercial, Colegio de Abogados de Medellín, Pág. 171.

puedan crear nuevas firmas y así facilitar el acceso a estos mecanismos a más parte de la población.

Del mismo modo la Ley 527 de 1999 no solo se encargó de definir las entidades de certificación, sino que igualmente estableció los parámetros y condiciones bajo las cuales podían ser conformadas, estableciendo que estas entidades podían ser privadas o públicas, de acuerdo con el capital con el cual fueran creadas; de origen nacional o extranjero, para lo que no existe restricción alguna al respecto ya que el fenómeno de globalización ha venido borrando aquellos límites para poder ser una de estas entidades de certificación, sin embargo estas entidades extranjeras deben cumplir con los mismos requisitos que le son exigidos a los nacionales; de igual manera se dispuso que estas entidades podían ser una persona jurídica común o incluso una Cámara de Comercio, así mismo la Ley 588 del 2000 estableció que los Notarios y Cónsules podían igualmente ejercer las función propias de las entidades de certificación³⁴.

Así mismo, las entidades de certificación fueron clasificadas en entidades abiertas y cerradas, entendiéndose por las cerradas, aquellas que se encargan de ejercer las funciones de certificación únicamente frente al suscriptor, sin recibir remuneración alguna a cambio por los servicios prestados, sobre lo cual el numeral 8 del artículo 1 del Decreto Reglamentario 1747 de 2000 señaló que es la entidad *“que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello”*, de tal manera que estos certificados conforme el artículo 4 del mencionado decreto deben señalar expresamente que el certificado solo tiene efectos entre la entidad certificadora y el suscriptor. Por su parte las entidades de certificación abiertas operan en sentido contrario a las cerradas, es decir, que la certificación no se limita a la entidad y el suscriptor, sino que tiene efectos respecto de todos aquellos que tengan algún tipo de interés en la certificación, estas entidades sí obtienen una remuneración por sus servicios y adicionalmente la actividad de certificación debe estar prevista en el objeto social de la entidad. Es necesario tener presente que los

³⁴ Cfr. RINCÓN CÁRDENAS, Erick. *“Aproximación Jurídica a la Firma Digital”*, Cámara de Comercio de Bogotá, Ed. Kimpres Ltda. 2008. Pág. 113.

certificados emitidos por la entidades de certificación cerrada no tienen los mismos efectos que la firma manuscrita, conforme al artículo 15 del Decreto 1747 de 2000.

4.1. Requisitos de las entidades de certificación.

Las entidades de certificación para poder operar deben cumplir con una serie de requisitos, lo cuales han sido clasificados en generales y específicos.

Con respecto a los requisitos generales, se anota que son aquellos que le son exigibles a todo tipo de entidad, así dentro de estos podemos encontrar:

- Capacidad
- Consentimiento
- Objeto lícito y causa lícita

Por su parte los requisitos especiales se refieren específicamente a aquellos que son exigidos a las entidades de certificación, y que le son propios por el objeto y funciones que van a desempeñar; estos requisitos han sido establecidos por el artículo 29 de la Ley 527 de 1999 modificado por el artículo 16 del Decreto 19 de 2012 de esta manera, las entidades de certificación deben contar como mínimo con una capacidad económica y financiera suficiente para realizar las actividades de certificación, así mismo deben contar con la capacidad y elementos técnicos necesarios que permitan el desarrollo de las actividades para las cuales fueron creadas, y por último sobre estas entidades recaen una serie de inhabilidades respecto de los representantes legales y los administradores para así generar seguridad en los usuarios; los requisitos se resumen en los siguientes puntos:³⁵

- **Capacidad económica y Financiera Suficiente:** No hay un criterio único en el que se pueda definir cuál debe ser el patrimonio mínimo que estas entidades deben tener, ya que se ha dicho que la capacidad económica no podría ser inferior a aquella que se le exige a una entidad del sistema financiero como a un Banco o a una Aseguradora, pues en todas estas entidades se encuentra en juego la confianza del público, además porque pueden llegar a incurrir en responsabilidad civil teniendo que cubrir con su patrimonio esta responsabilidad. De esta manera encontramos un vacío normativo pues no hay una regulación expresa que

³⁵ Cfr. Ibíd. Pág. 117-199

especifique cuál es el monto mínimo con el cual debe contar una entidad de certificación.

Sobre este punto el artículo 7 del Decreto 1447 de 2000, estableció a quienes se les puede exigir un patrimonio mínimo, disponiendo que *“Para determinar el patrimonio mínimo, sólo se tomarán en cuenta las cuentas patrimoniales de capital suscrito y pagado, reserva legal, superávit por prima en colocación de acciones y se deducirán las pérdidas acumuladas y las del ejercicio en curso. El patrimonio mínimo deberá acreditarse: 1. En el caso de personas jurídicas, por medio de estados financieros, con una antigüedad no superior a 6 meses, certificados por el representante legal y el revisor fiscal si lo hubiere. 2. Tratándose de entidades públicas, por medio del proyecto de gastos y de inversión que generará la actividad de certificación, conjuntamente con los certificados de disponibilidad presupuestal que acrediten la apropiación de recursos para dicho fin. 3. Para las sucursales de entidades extranjeras, por medio del capital asignado. 4. En el caso de los notarios y cónsules, por medio de los recursos dedicados exclusivamente a la actividad de entidad de certificación”*.Adicionalmente, con respecto a este requisito, la entidad de certificación debe cumplir con una de dos garantías: contratar un seguro o realizar un contrato de fiducia con patrimonio autónomo.

- **Capacidad y Elementos Técnicos necesarios:** La encargada de verificar este requisito es la Superintendencia de Industria y Comercio que ha delegado su función en una firma auditoria, firma que se encuentra regulada por la Resolución 26930 de 2000, sin embargo, esta firma de auditoría aún no ha sido creado, por lo cual normalmente las funciones de auditorías han sido ejercidas por firmas internacionales como Ernst & Young, adicionalmente no existe una normatividad en la cual se establezca cuales son los elementos técnicos específicos con los cuales deba contar una entidad de certificación.

Así mismo, el Decreto 1747 de 2000, dispuso que las entidades de certificación debían contar una infraestructura y unos recursos mínimos a fin de dar un cabal y correcto cumplimiento a sus funciones.

- **Inhabilidades para Representantes Legales y Administradores:** Los Representantes Legales y los Administradores de entidades de certificación no pueden haber tenido condenas penales salvo por delitos políticos o culposos, ni pueden haber sido suspendidos en su profesión por falta grave contra la ética, este requisito se ha creado fundamentalmente por la confianza que estas entidades deben generar en el público.

Vale la pena transcribir en este escrito, el artículo 30 de la Ley 527 de 1999 modificado por el artículo 161 del Decreto 19 de 2012, el cual establece las actividades a realizar por las entidades de certificación, para así generar una mayor claridad en cuanto a este tópico:

“Las entidades de certificación acreditadas por el Organismo Nacional de Acreditación de Colombia para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

- 1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.*
- 2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.*
- 3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.*
- 4. Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas.*
- 5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.*
- 6. Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas.*
- 7. Ofrecer los servicios de registro, custodia y anotación de los documentos electrónicos transferibles.*

8. Ofrecer los servicios de archivo y conservación de mensajes de datos y documentos electrónicos transferibles.

9. Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas".

Por otro lado, es pertinente hacer una explicación breve sobre los certificados digitales, certificados que son expedidos por estas entidades de certificación y los cuales necesitan para su emisión la creación previa de unas llaves, que de alguna manera podría decirse que se trata de unas llaves de seguridad, estas llaves son de dos tipos, una privada y otra pública, la llave pública de una persona la puede saber cualquier persona, puesto que esta solo sirve para encriptar el mensaje, es decir para cifrar el contenido de un documento de tal manera que solo pueda tener acceso a este la persona que tiene una clave privada con la cual descripta el contenido del documento. De esta manera, para crear seguridad y evitar que la clave se hackeada, la llave pública es entregada a la entidad de certificación, esta entidad le da a la persona un certificado en el que consta que la llave es de determinada persona y así esta persona envía a otra el mensaje con la llave pública y el certificado, para identificarse respecto de su firma³⁶.

Se debe tener presente, que la firma digital se certifica para generar una seguridad en el destinatario y en general en el público, este certificado lo que hace es identificar tanto a la entidad de certificación que lo emite como al suscriptor, la ley 527 dispone que este certificado contiene la clave pública, no obstante en algunas ocasiones prácticas el certificado puede llegar a contener la clave privada, elemento que no se incluye o no se tiene en cuenta en esta ley.

Por su parte, el artículo 35 de la ley 527, se encargó de establecer los contenidos mínimos que deben traer los certificados emitidos por las entidades de certificación, al respecto indicó:

“Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

³⁶ Fuente internet. <http://pendientedemigracion.ucm.es/info/cyberlaw/actual/1/con01-01-01.htm>

- 1. Nombre, dirección y domicilio del suscriptor.*
- 2. Identificación del suscriptor nombrado en el certificado.*
- 3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.*
- 4. La clave pública del usuario.*
- 5. La metodología para verificar la firma digital del suscriptor impresa en el mensaje de datos.*
- 6. El número de serie del certificado.*
- 7. Fecha de emisión y expiración del certificado”.*

Es del caso se debe tener en cuenta que estas entidades además de las funciones de certificación de firma digital pueden ejercer otro tipo de actividades como los son el estampado cronológico, según el cual se certifica que un mensaje de datos generado por un suscriptor no ha tenido variación o modificación alguna desde el momento en el cual el suscriptor realizó la solicitud de certificación, así mismo estas entidades pueden actuar como autoridad de archivo confiable, es decir ejercen la función de archivo de documentos electrónicos para que estos no se pierdan en el tiempo³⁷.

Antes de la expedición del Decreto 019 de 2013, al cual se hará referencia más adelante, toda actividad de certificación requería autorización del Estado, autorización que se daba por medio de la Superintendencia de Industria y Comercio (SIC), de esta manera la SIC no solamente se encargaba de dar esta autorización, sino que además debía velar por el funcionamiento de estas entidades y por el cumplimiento de las normas de competencia, por lo cual en caso que la SIC encontrara algún tipo de anomalía podía llegar incluso a imponer sanciones. No obstante lo anterior, estas facultades de la SIC fueron derogadas por medio del Decreto 019 de 2013, quien a su vez dispuso que el ente encargado de acreditar a las entidades de certificación debía ser el Organismo Nacional de Acreditación de Colombia, sin embargo la SIC continúa siendo el ente de control, inspección y vigilancia

³⁷ Cfr. Ibíd. Pág. 161-166

de las entidades de certificación, toda vez que el ente de Acreditación llamado ONAC a pesar de haber sido creado por el Decreto 4738 de 2008, como ente sin ánimo de lucro, de naturaleza mixta y constituido mediante documento privado, el mismo no se encuentra ejerciendo las funciones a su cargo.

Por otro lado, es necesario mencionar, que la ley 527 en cuanto a lo que respecta a las entidades de certificación, aún le falta regular una serie de aspectos que por el contrario si han sido objeto de regulación en otros países como Venezuela, Perú, entre otros, a título de ejemplo podemos mencionar que la ley Colombiana trae consigo un vacío normativo respecto de la suspensión del certificado y sus efectos. Sin embargo, si hizo referencia a temas cercanos como lo son la revocación del certificado, la terminación unilateral del vínculo entre la entidad de certificación y el suscriptor, pero hay ausencia de regulación respecto a la terminación específica de un certificado³⁸.

En conclusión se puede evidenciar que aunque la ley 527 de 1997 y el Decreto Reglamentario 1747 de 2000 trataron de ir más allá de la Ley Modelo de Comercio Electrónico de 1996 desarrollada por la CNUDMI, aún hace falta mayor regulación con la cual se pueda lograr una mayor especificidad en esta tema, ya que se puede evidenciar cómo las normas existentes establecen simplemente unos parámetros generales, a pesar que han sido varios los intentos en regular este tema.

³⁸ Cfr. Ibíd. Pág. 130

V. EL TRATADO DE LIBRE COMERCIO SUSCRITO ENTRE ESTADOS UNIDOS Y COLOMBIA Y SU INCIDENCIA EN LA LEGISLACIÓN SOBRE COMERCIO ELECTRÓNICO.

Como lo hemos venido anticipando en los capítulos anteriores, el Tratado de Libre Comercio suscrito entre Colombia y Estados Unidos – en adelante TLC –, además de sus múltiples implicaciones económicas, las cuáles no son objeto de análisis en el presente trabajo, también introdujo una serie de aspectos jurídicos en materia de autenticidad, que trascendieron el escenario bilateral del tratado, a tal punto que incidieron en la expedición de nuevas normas de carácter general que han permitido adecuar la legislación colombiana en materia de comercio electrónico a las necesidades del tráfico comercial actual. Así las cosas, el artículo 15.6 del TLC, titulado “Autenticación” consagró lo siguiente:

“Ninguna parte podrá adoptar o mantener legislación sobre autenticación electrónica que:

a) Prohíba a las partes en una transacción electrónica determinar en forma mutua los métodos apropiados de autenticación para dicha transacción; o

b) Impida a las partes tener la oportunidad de establecer ante las instancias judiciales o administrativas que la transacción electrónica cumple cualquier requerimiento legal con respecto a la autenticación.”

Como puede observarse, el TLC consagró más que una obligación o compromiso de un Estado contratante frente al otro, fue más allá y dispuso el imperativo de que los Estados parte debían abolir y no adoptar legislación que restringiera a las partes de una transacción electrónica adoptar de común acuerdo el método apropiado de autenticación.

De este modo tenemos que el TLC fue la génesis de la abolición de requisitos de autenticidad consagrados en la Ley 527 de 1999, abolición que se ha visto plasmada en el Código General del Proceso, el Decreto 2364 de 2012 y el Decreto 019 de 2012.

Ahora bien, hasta este punto hemos podido evidenciar las reformas introducidas por el Código General del Proceso en materia de autenticidad de mensajes de datos, siendo ahora

el turno de exponer los cambios implementados por el Decreto 2364 de 2012 y el Decreto 019 de 2012.

5.1. El Decreto 2364 de 2012 y la armonización del principio de equivalencia funcional plasmado en el artículo 7 de la Ley 527 de 1999.

El Decreto 2364 de 2012 reglamenta el artículo 7 de la Ley 527 de 1999, y en sus considerandos evidencia con claridad la influencia del TLC en su expedición:

“Que de conformidad con el artículo 15.6 del Tratado de Libre Comercio suscrito con los Estados Unidos de América, aprobado por la Ley 1143 de 2007, no se podrá adoptar o mantener legislación sobre autenticación electrónica que impida a las partes en una transacción electrónica determinar en forma mutua los métodos apropiados de autenticación o que les impida establecer, ante instancias judiciales o administrativas, que la transacción electrónica cumple con cualquier requerimiento legal con respecto a la autenticación.”

Resulta de vital importancia destacar que el Decreto 2364 de 2012 en concordancia con las obligaciones contraídas en virtud del TLC introduce en nuestro ordenamiento jurídico un esquema que podríamos denominar de “libre regulación en materia de autenticación”, toda vez que las partes dentro de un negocio jurídicos celebrado a través de medios electrónicos tendrán la facultad de determinar de manera libre los mecanismos de autenticación. Lo anterior sin lugar a duda implica un grado de evolución dentro de nuestra cultura jurídica, caracterizada por ser excesivamente reguladora y restrictiva de la libertad contractual. Prueba de ello son los inaplicables requisitos de autenticidad consagrados por la Ley 527 de 1999 en su concepción original, los cuáles ya tuvimos oportunidad de estudiar en capítulos anteriores. Así las cosas, aunque tome tiempo evidenciarlo en la práctica, nuestra legislación le ha dado un espaldarazo al principio de la buena fe y a la autonomía de la voluntad privada en las relaciones contractuales a través de la libre escogencia de métodos de autenticación.

De igual manera, este Decreto destaca la importancia de reglamentar la firma electrónica bajo un esquema de neutralidad tecnológica – sin privilegiar a la firma digital sobre otros

mecanismos de firma electrónica - para proveer seguridad jurídica a los negocios que se realicen a través de mensajes de datos:

“Que se hace necesario reglamentar la firma electrónica para generar mayor entendimiento sobre la misma, dar seguridad jurídica a los negocios que se realicen a través de medios electrónicos, así como facilitar y promover el uso masivo de la firma electrónica en todo tipo de transacciones.”

El profesor Nelson Remolina Angarita³⁹ destaca las bondades de este Decreto, en particular frente a la necesidad de hacer eficaz en la vida jurídica otros mecanismos de firma electrónica alternativos a la firma digital:

“Mediante el decreto 2364 del 22 de noviembre de 2012 el Gobierno Nacional reglamentó la firma electrónica del artículo 7 de la ley 527 de 1999. Con éste se deja en manos del país una alternativa de identificación electrónica diferente a la firma digital.

(...)

Inicia una nueva era respecto de las firmas en el mundo digital. También se despeja el oscuro y poco transparente discurso de marketing que idolatra ciegamente y a ultranza la firma digital (especialmente la certificada) como lo único jurídicamente válido.

Aunque la doctrina y la jurisprudencia ya habían mencionado esta clase de firma ello no era suficiente para generar mayor certeza jurídica sobre su uso en los negocios y la actividad estatal. Esto porque era constante el “ruido interesado” que algunos mercaderes de la firma digital realizaban.”⁴⁰

Como bien lo destaca el profesor Remolina Angarita, el Decreto 2364 de 2012 armoniza finalmente el principio de equivalencia funcional desarrollado por el artículo 7 de la Ley de Comercio Electrónico, el cual no obstante equiparar y no dar ningún trato preferencial a

³⁹ Profesor Asociado y Director de la Especialización en Derecho Comercial y del GECTI de la Facultad de Derecho de la Universidad de los Andes.

⁴⁰ REMOLINA ANGARITA, Nelson. “Primera reglamentación de la firma electrónica”. Diciembre 12 de 2012. Disponible en: http://gecti.uniandes.edu.co/docs/PRIMERA_REGLAMENTACION_FIRMA_ELECTRONICA.pdf

ninguna clase de firma electrónica, se veía restringido por el artículo 28 de la Ley 527 de 1999, el cual le daba un trato privilegiado a la firma digital.

En efecto, el Decreto 2364 acaba con dicho trato preferencial de la firma digital cuando en su artículo 5 consagra:

“Artículo 5. Efectos jurídicos de la firma electrónica. La firma electrónica tendrá la misma validez y efectos jurídicos que la firma, si aquella cumple con los requisitos establecidos en el artículo 3 de este decreto.”

Por su parte el artículo 3 del Decreto dispone:

“Artículo 3. Cumplimiento del requisito de firma. Cuando se exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan confiable como apropiada para los fines con los cuales se generó o comunicó ese mensaje.”

De la lectura de los dos artículos anteriormente citados podemos observar que queda abierta la posibilidad para que las partes adopten de común acuerdo el método de firma electrónica aplicable para su transacción – acuerdos EDI⁴¹ – y se establece como único requisito para que la firma electrónica sea admisible que el método empleado sea confiable.

Como si fuera poco lo anterior, el artículo 2 señala de manera expresa la igualdad de tratamiento entre firmas electrónicas:

“Artículo 2. Neutralidad tecnológica e igualdad de tratamiento de las tecnologías para' la firma electrónica. Ninguna de las disposiciones del presente decreto será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método,

⁴¹ El EDI (Electronic Data Interchange) es intercambio electrónico de datos de computadora a computadora entre Socios Comerciales (cadenas), con la finalidad de ahorrar tiempo al eliminar los tradicionales métodos de preparación y envío de documentos a través de mensajería. A la vez, tiene la ventaja de ser un método más seguro y confiable para el manejo de información. Disponible en: <http://www.masteredi.com.mx/SP/INFORMACION/que.asp>

procedimiento, dispositivo o tecnología para crear una firma electrónica que cumpla los requisitos señalados en el artículo 7 de la Ley 527 de 1999.”

La confiabilidad del método, cuando este es fruto de un acuerdo entre las partes de la transacción, se delimita de conformidad con lo dispuesto en el parágrafo del artículo 7 del Decreto 2364, en el sentido de señalar que la parte que suministre el mecanismo de firma electrónica deberá cerciorarse que sus mecanismos son técnicamente seguros y confiables, e incluso le impone la carga probatoria de acreditar dicha confiabilidad en caso de ser necesario.

Pero el Decreto 2364 no se limitó a señalar de una manera vaga que los mecanismos de firma electrónica deben ser técnicamente seguros sino que estableció “*criterios para establecer el grado de seguridad de las firmas electrónicas*” y al respecto señaló en su artículo 8 los siguientes, sin establecer un listado taxativo: (i) El concepto técnico emitido por un perito o un órgano independiente y especializado y (ii) La existencia de una auditoría especializada, periódica e independiente sobre los procedimientos, métodos o dispositivos electrónicos que una parte suministre.

No puede pasarse por alto, tal como lo señala el artículo 2 del Decreto, que para que cualquier método de firma electrónica sea admisible deben acreditarse todos los requisitos señalados en el artículo 7 de la Ley 527 de 1999, siendo la confiabilidad del método empleado, uno de los tres requisitos que deben cumplirse. El Decreto 2364 facilita la carga probatoria de la confiabilidad del método al señalar criterios para poder corroborarla.

De esta manera podemos concluir que el Decreto 2364 de 2012 se acopla a las exigencias establecidas por el TLC, por cuanto (i) permite a las partes pactar de mutuo acuerdo el mecanismo de firma electrónica a emplear en la transacción dotándola de autenticidad sin necesidad de acreditar requisitos de autenticidad adicionales (EJ: certificados digitales) – acuerdos EDI -, (ii) elimina el tratamiento preferencial de la firma digital y le da plenos efectos jurídicos a todos los mecanismos de firma electrónica, lo cual también se evidencia con la facultad que tienen las entidades de certificación desde la expedición del Decreto

Anti trámites de expedir certificado de firmas electrónicas y no solo certificados de firmas digitales, y (iii) reafirma la importancia de acreditar los requisitos consagrados en el artículo 7 de la Ley 527 de 1999 para la admisibilidad del mecanismo de firma electrónica, haciendo una regulación especial en cuanto al requisito de “confiabilidad del método” para el cual establece una serie de criterios que permitan a la parte que establece el método demostrar que el mismo es seguro.

5.2. El Decreto 19 de 2012 y la facultad de certificar firmas electrónicas.

Dentro del proceso de transformación que ha sufrido la legislación de comercio electrónico en nuestro país, consistente en adecuar los mecanismos de firmas electrónicas a las exigencias del comercio electrónico actual, encontramos una modificación muy importante introducida por el Decreto 19 de 2012, conocido como el Decreto “anti tramites”:

Dicha modificación consiste en atribuirle a las entidades de certificación la facultad de expedir certificados de firmas electrónicas y no solo de firmas digitales.

Como ya lo hemos manifestado a lo largo de este escrito una de las grandes críticas que se le ha hecho a la Ley 527 de 1999 es el tratamiento privilegiado atribuido a la firma digital, atentando contra el principio de equivalencia funcional consagrado en el artículo 7 de dicha ley. Uno de dichos tratos preferenciales consistía en que las entidades de certificación previamente autorizadas por la Superintendencia de Industria y Comercio solamente tenían la facultad de expedir certificados de firmas digitales. Dichos certificados digitales han sido considerados por nuestra práctica jurídica como el único mecanismo de acreditar la autenticidad de una firma digital plasmada en un mensaje de datos, dada la dificultad de acreditar mediante otros mecanismos los requisitos para la presunción de autenticidad establecidos en el artículo 28 de la Ley 529 de 1999. De lo anterior da cuenta la jurisprudencia⁴² de la Sala de Casación Civil de la Corte Suprema de Justicia que hemos citado en capítulos anteriores.

⁴² Cfr. CORTE SUPREMA DE JUSTICIA, Sala de Casación Civil, sentencia del 16 de diciembre de 2010. M.P. Pedro Octavio Munar Cadena.

El artículo 7 de la Ley 527 de 1999 establece como uno de los requisitos para que proceda la equivalencia funcional de la firma electrónica que se haya utilizado un método que permita identificar al iniciador de un mensaje de datos y que el contenido del mismo cuente con su aprobación, en otras palabras este requisito exige la acreditación de la autenticidad de la firma consignada en el mensaje de datos. De acuerdo con lo anterior, surge entonces el siguiente interrogante: ¿cómo puede probarse la autenticidad de un mensaje de datos?

De acuerdo con la versión original de la Ley 527 para poder acreditar la autenticidad de una firma digital se acudía a la expedición de un certificado digital por parte de una entidad autorizada de certificación – en Colombia la única autoridad autorizada de Certificación de carácter abierto es Certicamaras - pero entonces ¿cómo se satisfacía dicho requisito respecto a otros métodos de firma electrónica?, veamos:

“Infortunadamente, la preeminencia que las normas colombianas le dan a la firma digital parece dar cabida a especulaciones que niegan la validez y eficacia probatoria que tendría la firma electrónica.

Para despejar este equívoco es necesario hacer claridad sobre los conceptos. Firma electrónica es el género y se define como un “método adecuado” que permite identificar al iniciador de un mensaje de datos, de acuerdo con las condiciones particulares de éste. Por el contrario, la firma digital es la especie y consiste en un conjunto de datos incluidos en un mensaje de datos y obtenidos por conducto de la criptografía asimétrica, esto es, únicamente a través de las entidades de certificación. Es decir, hay dos posibilidades para lograr la autenticidad de un documento electrónico. La primera, consiste en suscribirse a una entidad de certificación y firmarlo digitalmente; la otra será utilizar un “método adecuado” por medio del que se pueda identificar a quien ha enviado un mensaje de datos.”⁴³(Subrayado como énfasis)

⁴³ QUIROZ GUTIERREZ, Marcos. “El papel de las entidades de certificación y la seguridad de la información y los derechos personales en el comercio electrónico”. Página 8. Bogotá, 2009.

La anterior cita es muy elocuente a la hora de exponer una realidad planteada por la ley 527 de 1999: solo las firmas digitales cuentan con un mecanismo para acreditar su autenticidad – el certificado digital – dejando a otras firmas electrónicas en la indefinición y vaguedad de establecer un “método adecuado” para poder satisfacer dicho requisito.

En pocas palabras la eficacia probatoria de un documento electrónico estaba en manos de las entidades de certificación, las cuáles de acuerdo con el artículo 30 de la Ley 527 de 1999, solo tenían la facultad de expedir certificados respecto de firmas digitales. Certificado que además en virtud del artículo 28 de dicha ley se había convertido en la práctica jurídica en un requisito *sine qua non* para la presunción de autenticidad de un mensaje de datos:

“De acuerdo con la Ley 527 de 1999 o de Comercio Electrónico, las Entidades de Certificación desempeñan un rol relevante en torno a la autenticidad e integridad de los documentos electrónicos, logrando la seguridad jurídica y, a su vez, la eficacia probatoria de este equivalente funcional del documento tangible. Son definidas como aquellas autorizadas para certificar firmas digitales, ofrecer o facilitar los servicios de registro y estampado cronológico de mensajes de datos, entre otras funciones relativas a las comunicaciones electrónicas.”⁴⁴(Subrayado como énfasis)

De acuerdo con lo expuesto en los párrafos anteriores, podemos evidenciar que las entidades de certificación tenían el poder de acreditar la eficacia probatoria de los mensajes de datos firmados mediante firma digital, dejando prácticamente inoperantes los demás mecanismos de firma electrónica los cuáles no podían ser susceptibles de certificación, y en consecuencia desprovistos de un mecanismo efectivo que pudiera avalar su autenticidad.

Teniendo claro este panorama desalentador para mecanismos de firma electrónica alternativos a la firma digital, veamos el valioso aporte realizado por el Decreto 019 de 2102.

⁴⁴ Ibídem. Pág. 4.

En efecto, el artículo 161 del Decreto 019 que modificó el artículo 30 de la Ley 527 de 1999 atribuyó a las entidades de certificación la facultad de expedir certificados respecto de firmas electrónicas, y no solo de firmas digitales:

“ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN

El artículo 30 de la Ley 527 de 1999, quedará así:

"Artículo 30. Actividades de las entidades de certificación. Las entidades de certificación acreditadas por el Organismo Nacional de Acreditación de Colombia para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas (...)"

De este modo tenemos entonces que gracias a la facultad que le atribuyó el Decreto 019 a las entidades de certificación de emitir certificados de toda clase de firmas electrónicas, se abre la posibilidad de dotar de eficacia probatoria a métodos alternativos de firma diferente a la firma digital. Así las cosas un “método adecuado” de firma electrónica podrá hoy en día probarse mediante un certificado, o mediante los criterios establecidos en el artículo 8 del Decreto 2364 de 2012.

Vale la pena mencionar que estas disposiciones son aplicables, de acuerdo con el artículo 2 del Decreto 019 a todas las actuaciones de los organismos de la Administración Pública que ejerzan funciones administrativas, lo cual significa que frente la administración pública podrá acreditarse la autenticidad de un mensaje de datos firmado mediante cualquier mecanismo de firma electrónica a través de un certificado. Ahora bien, frente actuaciones judiciales en donde sea aplicable el Código General del Proceso cualquier documento en forma de mensaje de datos tendrá presunción de autenticidad, presunción que entrará a regir a partir del 1 de enero de 2014.

Finalmente podemos concluir que el Decreto 019 de 2012 en armonía con el artículo 15.6 del TLC permite cumplir con el compromiso adquirido mediante dicho instrumento internacional en cuanto la posibilidad que tienen las partes de una transacción por medios electrónicos de “(...) *establecer ante las instancias judiciales o administrativas que la transacción electrónica cumple cualquier requerimiento legal con respecto a la autenticación.*”⁴⁵

⁴⁵ Artículo 15.6 del Tratado de Libre Comercio suscrito entre Colombia y Estados Unidos.

VI. LA CONTRATACIÓN ELECTRÓNICA.

En primer lugar, es preciso distinguir entre lo que se entiende por contrato electrónico y contrato informático, ya que la gran mayoría de las personas suelen confundir e indicar que son dos acepciones iguales, incurriendo en un error conceptual; así las cosas se debe entender por contrato electrónico “aquel que se realiza mediante la utilización de algún elemento electrónico, con influencia, decisiva, real y directa sobre la formación de la voluntad, el desenvolvimiento o la interpretación de un acuerdo; en general, se trata de aquella contratación que se celebra por medios electrónicos o teletemáticos”⁴⁶, por su parte el contrato informático es “el contrato que tiene por objeto bienes o servicios informáticos”⁴⁷. De esta manera, cabe resaltar que el objeto de estudio del presente capítulo hace referencia al concepto de contratación electrónica, es decir, aquella que se realiza por medios electrónicos.

Así las cosas, teniendo presente que este estudio se basa en la contratación electrónica, es menester tener en cuenta que los mecanismos de contratación hoy en día se han visto permeados por los canales electrónicos, los cuales la colectividad de las personas ha venido utilizando para agilizar las interacciones en el desarrollo del mercado. De esta manera las relaciones comerciales con el pasar de los días viene desarrollándose mediante la utilización de mecanismos electrónicos, conllevando necesariamente a que la contratación sea más especializada y se deje a un lado el diligenciamiento de una serie de documentos que dificultaban contraer vínculos contractuales.

Hoy en día, se evidencia que la contratación electrónica se ha venido implementando en gran medida en los mercados, toda vez que los clientes que adquieren bienes o servicios de terceros, han dejado de lado la eventual selección de un proveedor de acuerdo a las condiciones contractuales, y por el contrario ahora la elección corresponderá a la calidad del bien o servicio, marcas de los mismos, utilidad, entre otros aspectos, sin que el cliente tenga como parámetro de elección del productor las condiciones del contrato per se.

⁴⁶ RINCÓN CÁRDENAS, Erick. “Manual de Derecho de Comercio Electrónico y de Internet”, Ed. Universidad del Rosario. Bogotá, 2006. Pag 83 y 84.

⁴⁷ Ibídem. Pág. 84.

Teniendo en cuenta las facilidades de contratación que el mercado se encuentra ofreciendo, como es el referente a la contratación electrónica, se debe resaltar que este tipo de contratación presenta una serie de inconvenientes o preocupaciones, tales como la validez de la manifestación de la voluntad por parte del originador del mensaje de datos, la implementación de nuevos mecanismos para manifestar tal voluntad otorgando así la seguridad requerida por el mercado, la veracidad del originador del mensaje de datos, entre otros, aspectos que muy bien los ha traído al escenario el profesor Erick Rincón Cárdenas, así:

“En primer lugar, porque puede resultar muy difícil constatar que hay discernimiento de quien maneja una computadora; puede resultar bastante difícil verificar si se tuvo una intención real de obligarse, y puede resultar imposible probar que hay error, dolo o violencia en el consentimiento.

En segundo lugar, puede ocurrir que la declaración de voluntad sea automáticamente elaborada por una computadora y que la presencia de una persona no sea sólo mediata, al programar la computadora, pero no inmediata en el acto de celebración. Estas dificultades, sin duda alguna, transforman el consentimiento. En tercer lugar, es indudable que las nuevas tecnologías de las telecomunicaciones se relacionan con el fenómeno de la ampliación de los mercados, lo que nos sitúa ante la tarea pendiente de la unificación del derecho de las obligaciones y el de los contratos...”⁴⁸

Resulta claro entonces que las nuevas tecnologías traen consigo una serie de beneficios para el mercado y a su vez unos inconvenientes vistos desde la óptica estrictamente jurídica, tales como los enunciados anteriormente a saber, el conocimiento de la verdadera intención de los contratantes para la celebración del negocio jurídico y el no tener certeza de la efectiva manifestación de la voluntad de las partes. Del mismo modo, resulta indispensable conocer los efectos jurídicos que tiene la manifestación de la voluntad mediante la utilización del contrato electrónico, es decir, la manifestación del consentimiento para la adecuada formación del vínculo contractual.

⁴⁸ Ibídem. Pág. 82 y 83.

Conforme lo anterior, es menester traer a colación el concepto de equivalente funcional tratado en capítulos anteriores, toda vez que dicho principio facilita la contratación electrónica mediante la sustitución del soporte en papel físico por un mecanismo que soporte la voluntad de las partes en medios electrónicos. De esta manera “el documento electrónico, informático y teletemático es un documento con las mismas características, en principio y en cuanto a su validez jurídica, que cualquier otro de los que tradicionalmente se aceptan en soporte papel”⁴⁹ (Subraya fuera de texto), por lo que resulta claro entonces que el propio legislador al regular el comercio electrónico en Colombia, propendió por otorgar toda la validez jurídica a los actos que tengan como finalidad la celebración de un contrato por estos medios. Por su parte, el principio de equivalencia funcional fuera de otorgar y brindar validez legal a tales actos, permite que la manifestación de la voluntad en la oferta y aceptación del negocio que se pretende celebrar, goce de la validez y eficacia jurídica necesaria para dar seguridad al mismo sistema.

Así las cosas, la propia Ley 527 de 1999 que establece la validez de la contratación electrónica en el país, resulta completamente ajustada al ordenamiento legal colombiano, ya que abre la posibilidad de suscribir contratos por medios electrónicos, dotando dichos actos de validez jurídica por expresa disposición legal siempre y cuando se pueda constatar que se cumpla con los requisitos establecidos para prestar el consentimiento y perfeccionar el contrato a través de los procedimientos de oferta y aceptación de la misma, establecidos en los artículos 850, 851 y 864 del Código de Comercio⁵⁰; lo anterior, debido a que el ordenamiento legal colombiano no trae exigencias de forma para la celebración de contratos (salvo que verse sobre la adquisición de inmuebles o cualquier mueble sujeto a registro, caso en el que será necesario efectuar el registro del documento en la oficina correspondiente) sino habrá que velar por el cumplimiento de las condiciones del acto mismo.

Conforme lo anterior, a continuación se darán a conocer los elementos constitutivos de la manifestación de la voluntad y/o consentimiento para la formación de un contrato electrónico.

⁴⁹ Ibídem. Pág. 86.

⁵⁰ Ibídem. Pág. 88.

6.1. El consentimiento electrónico, la oferta y su aceptación.

El consentimiento o manifestación de la voluntad para la celebración de contratos electrónicos, es uno de los aspectos que trae implícitos problemas referentes al perfeccionamiento del contrato mismo, ya que no es claro identificar donde, como, cuando queda perfeccionado el contrato, lo que da lugar a que este tipo de contratación se vea inestable y no pueda brindar la seguridad jurídica requerida para el sistema; de ahí que surjan interrogantes tales como ¿Qué pasa si la persona que acepta una oferta es incapaz? ¿Cómo sabemos que tanto la oferta como la aceptación son serias? ¿Quién representa a las partes en este tipo de negociación? ¿Qué procedencia tienen los bienes que se ofrecen en una página de internet?, entre muchos otros que sin lugar a dudas conllevan a imaginar que este tipo de contratación no pueda llevarse a cabo.

De esta manera, y teniendo en cuenta la diversidad de problemáticas que enfrenta la contratación electrónica, debemos indicar que “... *para que el consentimiento expresado electrónicamente sea válido, las partes deben ser capaces, lo cual, en materia de negocios electrónicos, implica serias dificultades, teniendo en cuenta que las partes nunca están en presencia de la otra.*”⁵¹, por lo que la validez otorgada a todo mecanismo digital mediante el que se manifiesta la voluntad de cada uno de los contratantes, es perfectamente viable una vez cada uno de los intervinientes pueda manifestar voluntariamente su intención de celebrar tal acto o negocio jurídico.

Resulta claro que la contratación electrónica tiene un problema en particular referente a la validez de la manifestación de voluntad de cada una de las partes para la celebración del negocio jurídico, toda vez que de no haber certeza respecto de la verdadera manifestación de la voluntad de cada una de las partes, puede presentarse el evento de tener un mecanismo susceptible de defraudaciones electrónicas, es decir, de tener personas ajenas al sistema que aparentemente manifiestan la voluntad de una de las partes abusivamente por medio de Hackers, entre otros.

Debido a las dificultades relacionadas con la manifestación de voluntad, resulta necesario definir los conceptos de oferta electrónica y aceptación electrónica, donde el concepto

⁵¹ Ibídem. Pág. 89.

inicialmente mencionado hace referencia a la propuesta que se da a otra persona para la celebración de un negocio jurídico, y la aceptación se tendrá como aquella aquiescencia de la oferta inicialmente presentada, sin que se haga aclaración o adición alguna ya que se transformaría en una contraoferta, en este orden de ideas, se hará alusión al distinguido al doctor Cárdenas quien en su obra titulada “manual de derecho de comercio electrónico y de internet”, define estos conceptos de la siguiente forma:

- **Oferta Electrónica:** *“declaración unilateral de voluntad que una persona realiza a través de medios de comunicación y/o medios informáticos al invitar a otra persona a la celebración de una convención que quedará perfecta con la sola aquiescencia de ésta”*⁵².
- **Aceptación Electrónica:** *“aquella declaración unilateral de voluntad que una persona realiza a través de medios de comunicación y/o medios informáticos, donde se manifiesta su conformidad a una propuesta recibida por ella”*⁵³.

Así las cosas, estos conceptos sin lugar a duda, son los elementos esenciales para la manifestación del consentimiento en la celebración de cualquier negocio jurídico, ya que la simple unión de los mismos se traduce en el consentimiento de las partes para la finalidad deseada por ellas, es decir, la celebración del contrato o negocio jurídico. De esta manera, resulta necesaria la aplicación de las disposiciones legales colombianas respecto a la oferta y aceptación de la misma, es decir, se debe cumplir con el principio del derecho que señala que “la aceptación debe darse mientras la oferta esté vigente, de manera oportuna y debe ser pura y simple”⁵⁴, circunstancias que se observarán en la manifestación del consentimiento del agente y que permiten tener certeza de su voluntad.

A simple vista parece fácil la consecución de un negocio jurídico por los canales electrónicos, sin embargo este tipo de manifestaciones de la voluntad se han visto enfrentadas a los problemas que la contratación cotidiana y conocida por todos ha tenido que solucionar, por lo que resulta aplicable toda la normatividad legal vigente, particularmente a las disposiciones del Código de Comercio que plantean solución a este tipo de inconvenientes; a título de ejemplo está el problema referente al lugar donde se

⁵² Ibídem. Pág. 90.

⁵³ Ibídem. Pág. 91.

⁵⁴ Ibídem. Pág. 92.

entiende se ha formado el contrato, para lo cual el artículo 864 del Código de Comercio a dispuesto que será en la residencia del oferente, disposición que facilitó la negociación del contrato y permitió dejar las reglas claras entre los contratantes respecto a la ley aplicable, y por lo tanto las demás disposiciones legales colombianas serán aplicables para la suscripción de negocios mediante la utilización de mecanismos digitales.

Por su parte, la Ley 527 de 1999 en su artículo 14 implementó una regla consistente en que la oferta y aceptación tienen expresa validez o fuerza probatoria cuando hayan sido expresadas por medio de un mensaje de datos, del mismo modo el artículo 15 dispuso que no se negaran efectos jurídicos a las relaciones que se lleven a cabo entre el iniciador de un mensaje de datos y el destinatario del mismo; conforme en tales disposiciones, es clara la voluntad del legislador para otorgar la validez necesaria a los actos celebrados por estos medios, donde al utilizar estos instrumentos para manifestar la voluntad, se entiende que la misma goza de plena validez, situación que genera certidumbre, confianza y seguridad que los contratantes han buscado para poder suscribir este tipo de contratos.

Ahora bien, teniendo en cuenta la seguridad jurídica que las anteriores disposiciones pretendieron dar al sistema, debemos dar claridad a que la utilización de nuevas tecnologías y su respectiva implementación a la vida de las personas, necesariamente genera una serie de inconvenientes tales como los que líneas arriba se mencionaron, aun así el ordenamiento legal actual es claro en que la manifestación de la voluntad por canales electrónicos goza de plena validez jurídica siempre y cuando se haya realizado a través de mensajes de datos o algún otro instrumento que sea equivalente.

Para dar solución a aquellos inconvenientes que fueron resaltados al inicio de este capítulo, vemos que las legislaciones del mundo han establecido el principio de “no repudio”, que se expresa de la siguiente manera:

“No repudio o irrefutabilidad: Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación. En el caso de no repudio de origen, el remitente del mensaje no puede negar haberlo enviado. En

caso de no repudio de destino, el destinatario del mensaje no puede negar haberlo recibido”⁵⁵.

Este principio obra adecuadamente para brindar al sistema de contratación electrónica la seguridad que se requiera, toda vez que aquella persona que envía o recibe una oferta, no puede decir que no ha sido remitida por ella, ya que al demostrar que la contraparte actuó en el negocio o tratativas, automáticamente queda vinculada al mismo, imposibilitando así indicar que no es la manifestación de su voluntad ya que se ha realizado por un medio electrónico, ya que hay “un sistema de información programado por el iniciador o en su nombre para que opere automáticamente”⁵⁶, es decir, el mensaje es respondido por la persona misma o por una orden que esta le ha dado al sistema previa programación, que en ultimas es la misma persona y por lo tanto no hay lugar a duda alguna respecto de la identificación del originador del mensaje.

Conforme lo anterior, el sistema ha diseñado y establecido unas entidades de certificación que tienen como finalidad dar fe que las partes que se encuentran negociando son aquellas que se han registrado en el sistema, permitiendo así confiar en que al otro lado de la negociación hay una persona que efectivamente se encuentra manifestando la voluntad, por tal motivo, las entidades de certificación son de vital importancia en la celebración de negocios o contratos electrónicos, ya que son las encargadas de brindar la seguridad jurídica necesaria en la negociación contractual y así permitir el desarrollo jurídico tecnológico del caso.

Por su parte, el sistema aun no prevé la problemática de la capacidad de cada una de las partes que se encuentra en una negociación por canales electrónicos, ya que en el evento en que “no podamos cerciorarnos con una entidad de certificación, o nos sea difícil obtener información veraz sobre la capacidad de la contraparte, como puede ocurrir cuando el negocio se está realizando en dos lugares o países distintos. Esta, tal vez, es una problemática que el comercio electrónico no ha podido solucionar dado que, para esto se necesitaría prácticamente la existencia de una entidad certificadora de carácter

⁵⁵ RINCÓN CÁRDENAS, Erick. “Aproximación jurídica a la firma digital y a los prestadores de servicios de certificación digital”. Cámara de Comercio de Bogotá. 2008. Pág. 205.

⁵⁶ Ibídem. Pág. 206.

internacional, que agrupara la información de todos los operadores, y ni que hablar respecto de los usuarios que hagan uso de la contratación electrónica, ya que velar por la capacidad de cada uno de estos sería prácticamente imposible.”⁵⁷, sin embargo, a pesar de no contar con un sistema que nos dé cien por ciento de seguridad para conocer si la contraparte tiene o no la suficiente capacidad para contratar, el sistema legal si contiene un principio fundamental que conocemos como buena fe, principio mediante el que se confía en el buen actuar del otro y se espera que se este manifestando cualquier voluntad de manera autónoma, y que será aplicable a todo tipo de relación y que permite otorgar un respiro al sistema de contratación electrónica.

Ahora bien, el profesor Cárdenas ha mencionado que “para que una persona realice una manifestación de voluntad por medios electrónicos, es porque tiene conocimiento de éstos tales como navegar en internet, usar correo electrónico, usar servicios PSC etc.”⁵⁸, por lo que resulta apenas obvio que el agente tiene plena capacidad para manifestar su voluntad, dado que si se tiene la capacidad para hacer uso de todas las herramientas tecnológicas, también la tendrá para manifestar su voluntad para la celebración de un negocio jurídico, y por lo tanto no quedaría con excusa alguna para indicar con posterioridad a la emisión del mensaje de datos que no tenía la capacidad para acceder a estos mecanismos electrónicos y mucho menos respecto a la manifestación de la voluntad en el mensaje de datos.

Así las cosas, una vez resueltos aquellos interrogantes que al inicio del presente capítulo se formularon, se evidencia que tanto la oferta como la aceptación de la misma forman parte del consentimiento y de la manifestación de la voluntad para llegar al negocio jurídico deseado por las partes, por lo que resulta que el sistema de contratación electrónica fuera de tener unas entidades de certificación, se inspira en gran medida en una confianza y apariencia basada en la buena fe de los contratantes respecto al negocio a celebrar.

El profesor Erick Rincón Cárdenas, ha señalado unos principios jurídicos en que se fundamenta el consentimiento electrónico, los cuales son la confianza y la apariencia; “desde el punto de vista del oferente, no resulta obligado por su voluntad, sino por la apariencia jurídica creada; se trata de un fenómeno imputativo de efectos negociales con

⁵⁷ Ibídem. Pág. 209.

⁵⁸ Ibídem. Págs. 209 y 210.

base en la regla de la primacía de lo declarado por sobre las intenciones. Desde el punto de vista del aceptante, no interesa tanto su voluntad, como la confianza que prestó para aceptar”⁵⁹, de esta manera, se evidencia que más que la voluntad hay que partir de la base de la apariencia que del acto de a conocer el oferente, lo que permite evidenciar que tan veraz es el mismo desde todo punto de vista, y una vez se tenga una aproximación de lo que se está ofertando será responsabilidad del aceptante acceder a tal ofrecimiento lo que se refleja en la confianza que esa oferta le ha generado.

Por su parte, los anteriores principios van de la mano con la efectiva manifestación de la voluntad por cada uno de los contratantes en la relación jurídica que se pretende implementar, ya que tal manifestación de voluntad permite que se configure el consentimiento en el acto o negocio jurídico, lo que se inspira en una propuesta (oferta) y el acceder a dichas condiciones (aceptación), siempre bajo el supuesto de una confianza en el otro.

Teniendo claro el interrogante de cómo aplicaría la oferta y la aceptación de la misma en la manifestación de voluntad, sobra mencionar que el sistema legal colombiano, particularmente la Ley 527 de 1999 consagra que toda actuación o manifestación de la misma para consolidar el consentimiento tiene y goza de todas las prerrogativas legales para que genere efectos en el mundo jurídico, claro está siempre que se cumpla con los lineamientos que el estatuto comercial trae consignados respecto a la manifestación tanto de la oferta como la aceptación de esta, ya que es la norma que suple los eventuales vacíos jurídicos que deja la “Ley de Comercio Electrónico”, por lo que resulta completamente viable y procedente realizar una contratación por medios electrónicos, y de esta manera habría un escenario ideal para el desarrollo de los nuevos instrumentos que nos ha venido proporcionando las nuevas tecnologías, caso en el que la ciencia jurídica no puede verse rezagada por estas tecnologías y por lo tanto se debe adecuar a las nuevas exigencias de los mercados.

⁵⁹ RINCÓN CÁRDENAS, Erick. “*Manual de Derecho de Comercio Electrónico y de Internet*”, Ed. Universidad del Rosario. Bogotá, 2006. Pág. 95 y 96.

VII. CONCLUSIONES.

A lo largo de este trabajo se pudieron plantear algunos aspectos esenciales que hacían que la Ley de Comercio Electrónico fuera anticuada frente a las realidades del comercio electrónico actual, caracterizado por la celeridad en las transacciones y en hacer de las herramientas jurídicas sobre la materia un aspecto que facilite y no entorpezca su dinámico desarrollo.

De esta manera vimos como la primera iniciativa en este tema estuvo dada por la ley modelo sobre comercio electrónico de la Comisión de las Naciones Unidas para el desarrollo del derecho mercantil internacional (CNUDMI), ley que se inspiró en la realidad y necesidades que se venían presentando en el comercio. Por su parte, en Colombia se expidió la ley 527 de 1999 *“Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”*, esta ley tomó la esencia de la ley modelo de la CNUDMI copiando algunos de sus artículos complementándola con una regulación adicional, pues tocó temas de los cuales la ley modelo no se encargó como por ejemplo el tema de las entidades de certificación.

Así las cosas la regulación en Colombia no se detuvo con la Ley 527 de 1999, sino que por el contrario son varias la normas que han sido expedidas en nuestro país a fin de continuar con una regulación que contenga una mayor especificidad sobre este tema y con esto evitar vacíos normativos, sin embargo es de anotar que a pesar de los constantes intentos aún la normativa sobre comercio electrónico no es suficiente.

Con relación a quienes pueden actuar como autoridad de certificación y los requisitos que se deben cumplir para ejercer las actividades propias de estas entidades, son dos aspectos que sin lugar a duda brindan la seguridad jurídica requerida para la negociación mediante la utilización de los mensajes de datos.

De acuerdo a lo anterior, se evidencia que la Ley 527 de 1999 introdujo al sistema legal colombiano un principio consistente en la Equivalencia Funcional, que ha sido desarrollado principalmente por el artículo 7 de la referida ley, sin embargo, dicho concepto se complementó con los artículos 6 y siguientes. Es fundamental hacer mención que este principio es en esencia el que le da origen a la contratación electrónica en nuestro país, toda vez que es el que permite salir de la cotidianidad en cuanto a la firma de contratos en papel físico, conllevando necesariamente a que se pueda tramitar los negocios jurídicos en mensajes de datos u otros documentos equivalentes que brinden la seguridad necesaria para los contratantes.

La Equivalencia Funcional fuera de ser un principio por medio del que se inspira el comercio electrónico, es una herramienta que sin lugar a dudas se adecua a las necesidades actuales de las relaciones interpersonales de las personas, es decir, es una reacción del sistema a los cambios informáticos, toda vez que el negocio jurídico debe poderse llevar a cabo por otros instrumentos fuera de los que comúnmente se conocen para la celebración de un negocio.

Así mismo, se evidencia que la Ley 527 de 1999 además de traer a colación el comercio electrónico, facilita ampliamente la celebración de un negocio jurídico o contrato, toda vez que gracias a la Equivalencia Funcional, hay nuevas maneras de manifestar la voluntad para llegar al acuerdo requerido, el consentimiento de las partes se ve reflejado en la indefectible firma que las partes imponen en un documento, mensaje de datos, correo electrónico, entre otros. Es de resaltar que tanto la oferta como la aceptación de la misma, contribuyen al acuerdo entre las partes, las cuales se pueden manifestar mediante la utilización de la firma en un simple mensaje de datos, claro está, siempre que se acredite la veracidad de los mismos y la fuerza probatoria que de los mismos se pueda derivar, para lo que nuestra legislación ha implementado instituciones como la de Entidades de Certificación.

Por otro lado, propusimos como principal falencia de la Ley de Comercio Electrónico el tratamiento privilegiado otorgado a la firma digital a la cual le atribuyó una regulación especial en materia de presunción de autenticidad y la posibilidad de ser certificada por

Entidades de Certificación autorizadas, atribuciones que no otorgó a otras firmas electrónicas, dejándolas en consecuencia sin eficacia probatoria, aspecto que resultaba contradictorio frente al principio de equivalencia funcional desarrollado por la misma Ley en su artículo séptimo. Al respecto pudimos evidenciar la posición de la Corte Suprema de Justicia Colombiana y de algunos doctrinantes sobre la materia.

De igual manera pudimos apreciar cómo la legislación colombiana ha ido supliendo los anteriores defectos, mediante la expedición de normas que dotan de presunción de autenticidad a los mensajes de datos – Código General del Proceso -, atribuyen los mismos efectos jurídicos a cualquier mecanismo de firma electrónica que cumpla con los requisitos del artículo séptimo de la Ley 527 de 1999 – Decreto 2364 de 2012 – y la facultad otorgada a las entidades de certificación de emitir certificados de firmas electrónicas y no solo digitales – Decreto 019 de 2012 -.

Por último y para finalizar es menester indicar que la Ley de Comercio Electrónico (Ley 527 de 1999) introdujo al sistema legal colombiano un mecanismo que facilita en gran medida el desarrollo de las relaciones comerciales en el mercado, ley que se ha expedido en respuesta de los cambios que han venido implementando los comerciantes de acuerdo a la implementación de nuevos sistemas informáticos que permean la celebración de negocios jurídicos.

VIII. BIBLIOGRAFÍA.

- RINCÓN CÁRDENAS, Erick. “Manual de Derecho de Comercio Electrónico y de Internet”, Ed. Universidad del Rosario. Bogotá, 2006.
- RINCÓN CÁRDENAS, Erick. “Aproximación jurídica a la firma digital y a los prestadores de servicios de certificación digital”. Cámara de Comercio de Bogotá. 2008.
- <http://web.certicamara.com/media/69109/validez%20y%20seguridad.pdf>.
- <http://www.masteredi.com.mx/SP/INFORMACION/que.asp>.
- http://www.sela.org/attach/258/default/Di-7-12_Fundamentos_Firma_Digital_y_su_Estado_Arte_en_ALC-Final.pdf
- PEREZ, Marco. "El tratamiento legal de la firma electrónica en Colombia y en el derecho uniforme". Revist@ e – Mercatoria Volumen 1, Número 1. Bogotá, 2002.
- <http://lema.rae.es/drae/?val=firma>
- CORTE CONSTITUCIONAL. Sentencia C-662 de 2000. M.P. Alejandro Martínez Caballero.
- CORTE CONSTITUCIONAL, sentencia C – 622 de 2000 M.P. Fabio Morón Díaz.
- CORTE CONSTITUCIONAL, sentencia C – 831 de 2001. M.P. Álvaro Tafur Galvis.
- CORTE SUPREMA DE JUSTICIA, Sala de Casación Civil. Sentencia del 20 de octubre de 2005. M.P. Pedro Octavio Munar Cadena.
- CORTE SUPREMA DE JUSTICIA, Sala de Casación Civil. Sentencia del 16 de diciembre de 2010. M.P. Pedro Octavio Munar Cadena.
- CONSEJO DE ESTADO, Sala de Consulta y Servicio Civil. Rad. 1989 Sentencia del 18 de marzo de 2010. Consejero Ponente. Enrique José Arboleda Perdomo.
- QUIJANO PARRA, Jairo. “Manual de derecho probatorio.” Ediciones Librería Profesional, Bogotá, 2002.
- MENDÍVIL, Ignacio. “ABC de los documentos electrónicos seguros”. Página 3. México, 1999.

- HENAO RESTREPO, Darío. “Ley de Comercio Electrónico en Colombia (ley 527 de 1999)” en Nuevos Retos del Derecho Comercial, Colegio de Abogados de Medellín.
- <http://pendientedemigracion.ucm.es/info/cyberlaw/actual/1/con01-01-01.htm>
- REMOLINA ANGARITA, Nelson. “Primera reglamentación de la firma electrónica”. Diciembre 12 de 2012. Disponible en: http://gecti.uniandes.edu.co/docs/PRIMERA_REGLAMENTACION_FIRMA_ELECTRONICA.pdf
- <http://www.masteredi.com.mx/SP/INFORMACION/que.asp>
- QUIROZ GUTIERREZ, Marcos. “El papel de las entidades de certificación y la seguridad de la información y los derechos personales en el comercio electrónico”. Bogotá, 2009.
- Tratado de Libre Comercio suscrito entre Colombia y Estados Unidos.