

REPUBLICA DE COLOMBIA
PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE CIENCIAS JURIDICAS Y SOCIOECONOMICAS

NUEVAS TENDENCIAS DE LA PRUEBA
Ley de Comercio Electrónico

TESIS DE GRADO PARA OPTAR AL TITULO DE ABOGADO

JUAN CARLOS HOYOS
LEOPOLDO RUIZ DEL VALLE

Bogotá, D.C., Mayo de 2.001

AGRADECIMIENTO

Nuestro sincero agradecimiento al doctor Edgar Munévar Arciniegas, compañero de estudios, amigo incomparable, quien nos ayudó para tomar la decisión de elaborar el presente trabajo, y nos orientó en el desarrollo del mismo.

**A mis padres.
A Alejandro y María Camila, mis hijos adorados,
quienes con su alegría, ternura y amor
me llevaron a graduarme finalmente.**

Leopoldo.

A mis padres.

Juan Carlos

TABLA DE CONTENIDO

	Pág.
Introducción	
1. Prueba Documental	1
1.1 Según el autor	2
1.2 Según la grafía	8
1.3 Según la materia	9
1.4 Según el contenido	10
2 Disposiciones Generales Ley 527 de 1.999	12
2.1 Ambito de Aplicación	12
2.2 Definiciones	13
2.3 Interpretación	15
2.4 Modificación mediante acuerdo	15
2.5 Reconocimiento jurídico de los mensajes de datos	16
2.6 Escrito	17

2.7 Firma	17
2.8 Original	18
2.9 Integridad de un mensaje de datos	18
2.10 Admisibilidad y fuerza probatoria de los mensajes de datos	19
2.11 Criterio para valorar probatoriamente un mensaje de datos	19
2.12 Conservación de los mensajes de datos y documentos	20
2.13 Conservación de mensajes de datos	20
3.1 Formación y validez de los contratos	21
3.2 Reconocimiento de los mensajes de datos por las partes	21
3.3 Atribución de un mensaje de datos	22
3.4 Presunción del origen de un mensaje de datos	22
3.5 Concordancia del mensaje de datos enviado y recibido	23
3.6 Mensajes de datos duplicados	23
3.7 Acuse de recibo	23
3.8 Efectos jurídicos	24
4 Comercio electrónico en materia de transporte de mercancías	25
4.1 Actos relacionados con los contratos de transporte de mercancías	25
4.2 Documentos de Transporte	26
5 Firmas digitales, certificados y entidades de certificación	27
5.1 Firmas digitales	27

5.2 Entidades de certificación	28
5.3 Certificados	31
5.4 Suscriptores de firmas digitales	33
6. Superintendencia de Industria y Comercio	34
6.1 Funciones de la Superintendencia de Industria y Comercio	34
6.2 Sanciones	35
7 Disposiciones varias	37
7.1 Certificaciones recíprocas	37
7.2 Incorporación por remisión	37
8 Decreto 1747 de 2.000	38
8.1 Aspectos Generales	38
8.2 De las entidades de certificación y certificados digitales	40
8.3 Facultades de la Superintendencia de Industria y Comercio	57
9 Resolución No. 26930	59
9.1 Entidades de certificación cerradas	59
9.2 Entidades de certificación abiertas	61
9.3 Certificados	76
10 Sentencia 662 de 2.000	76
10.1 Generalidades	76
10.2 La demanda	77

10.3 Intervenciones ciudadanas y de autoridades públicas	79
10.4 Concepto del procurador general de la nación	84
10.5 Consideraciones y fundamentos	85
Conclusiones	100
Citas bibliográficas	116
Bibliografía	118

INTRODUCCION

Pretendemos analizar la nueva ley de comercio electrónico o Ley 527 de 1.999, pues a nuestro modo de ver es uno de los más importantes cuerpos legislativos expedidos en los últimos años en Colombia.

El mundo moderno, ágil y rápido en comunicaciones, necesita regular las relaciones surgidas entre las personas. El empleo creciente del Internet,

computadores, fax, correo electrónico y muchos otros medios de comunicación inmediata, requiere que los usuarios de estos medios, tengan certeza y amparo jurídico para lograr la confianza y la seguridad en las relaciones comerciales que con ocasión de la utilización de estos medios puedan surgir.

El esquema que proponemos al hacer el análisis exhaustivo de éste tema, parte de un estudio acerca de los documentos, para posteriormente adentrarnos en la Ley 527 de 1.999, el decreto 1747 de 2.000 y la Resolución 26930 de 2.000.

Posteriormente analizaremos la Sentencia de la Corte Constitucional No. 662 de 2.000, mediante la cual la Corte Constitucional declara exequibles los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1.999.

Dentro del análisis propuesto, estudiaremos el aspecto netamente jurídico de la Ley y su legislación complementaria, para terminar con los motivos que llevaron a la Corte Constitucional a declarar la exequibilidad de los artículos mencionados anteriormente de la Ley 527 de 1.999.

En un mundo permanentemente en movimiento hacia el progreso y hacia la rapidez en la toma de decisiones de toda índole, el derecho debe adecuarse a ese

ritmo y ser instrumento para generar confianza entre las personas que día a día utilizan estos medios electrónicos para realizar sus negocios e inversiones.

Colombia es uno de los países que están a la vanguardia con la expedición de la Ley 527 de 1.999 y toda su legislación complementaria. Bien por Colombia y enhorabuena por nosotros al tener la oportunidad de analizar la nueva legislación en materia de Comercio Electrónico.

1. PRUEBA DOCUMENTAL

Conforme al artículo 251 del Código de Procedimiento Civil, “*son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga el carácter de representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares*”.

Doctrinariamente, podemos encontrar dos tendencias acerca de los tipos de documentos que existen. Así, los civilistas lo estudian bajo una dogmática histórica y formalista, mientras que los procesalistas, los analizan en forma mucho más elástica y funcional.

Así, SCHULTZE, empieza entendiendo como documento todo objeto corporal que presenta trazas de una humana actividad dirigida a consignar una noticia, como monumentos, monedas, sellos, etc., concluye, desde el punto de vista jurídico, constriñendo esta especie al solo escrito en el cual se ha fijado un pensamiento a través de palabras (1).

Para los procesalistas, en cambio, el documento tiene dos significados. En sentido tradicional, aquel en que consta por escrito una expresión del pensamiento. En sentido amplio, es todo objeto que enseña una representación del pensamiento, no siempre escrito, o una representación cualquiera, como hitos, fotografías, tallas.(2). GUASP dice: ...existen, y cada vez más, en más número, otros objetos que sin ser escritos, documentan y acaso con mayor fidelidad que el escrito mismo...(3).

Hechas las anteriores precisiones acerca de los documentos, podríamos intentar una clasificación de ellos, muy acorde con la expuesta por Luis Muñoz Sabaté, quien atendiendo a cuatro circunstancias específicas los clasifica según su autoría, grafía, materia y contenido.

1.1. SEGÚN EL AUTOR:

El autor, es la parte más importante del documento, porque le da vida material. Sin él, el documento no podría existir. Surge así, con base en la calidad del autor una primera distinción entre documento privado y documento público.

1.1.1. DOCUMENTO PUBLICO:

Según el artículo 251 del Código de Procedimiento Civil en sus incisos 2º. Y 3º., “ Documento público es el otorgado por el funcionario público en ejercicio de su cargo o con su intervención. Cuando consiste en un escrito autorizado o suscrito por el respectivo funcionario, es instrumento público; cuando es otorgado por un notario o quien haga de sus veces y ha sido incorporado en el respectivo protocolo, se denomina escritura pública”.

Así, vemos que los documentos públicos se dividen en documentos públicos en general e instrumentos públicos, denominación que corresponde a “los documentos autorizados por notario competente en que se constituyen , reconocen, modifican o extinguen relaciones jurídicas entre partes, o en que se consignan hechos relacionados con el derecho y cuya memoria conviene conservar”(4).

1.1.2. DOCUMENTO PRIVADO:

Al tenor del artículo 251 del Código de Procedimiento Civil, “Documento privado es el que no reúne los requisitos para ser documento público”.

Como bien se puede apreciar, la definición de documento privado es bastante amplia.

1.1.3. “No obstante lo anterior, nuestra Honorable Corte Suprema de Justicia, en sentencia de 8 de Octubre de 1.997, estableció ciertas características que deben reunir tanto los documentos públicos como los privados:

1.1.3.1. La fecha: que tiene valor probatorio “adversus omnes” cuando el documento es público, y solo entre las partes, cuando el instrumento es privado.

1.1.3.2. La parte dispositiva: constituida por el conjunto de disposiciones de quienes conforman la esencia del acto allí contenido, las que se presumen veraces entre ellos y los obliga mientras no se pruebe lo contrario.

1.1.3.3. La parte enunciativa: que consiste en las aseveraciones accesorias por medio de las cuales se indican los acontecimientos preliminares del suceso, o se mencionan circunstancias no esenciales del mismo, manifestaciones que, por ende, de no existir, la sustancia del asunto no resultaría menguada por su ausencia”.(5).

Dice la Corte que las anteriores enunciaciones pueden guardar o no relación con las disposiciones contenidas en el documento. En caso que

la relación sea directa deberá haber cierta armonía que permita que la fe de la cual esté dotado el instrumento, las abarque conjuntamente y de manera indivisible, es decir, sin que haya posibilidad de atribuir eficacia demostrativa al hecho desfavorable desligándolo de las adiciones o explicaciones favorables que estén íntimamente vinculadas; todo esto fundamentado en el artículo 258 del Código de Procedimiento Civil.

Por otro lado, la Corte ha dicho que no obstante lo que las partes declaren en un documento público, cuando una de ellas alega que es otro su contenido, podrá acudir a la prueba de testigos, y, en forma general, a todos los medios que le permitan llevar al convencimiento del juez la verdad; prevaleciendo ésta sobre el acto público.

Lo anterior no es contrario a lo que dispone el artículo 256 del Código de Procedimiento Civil, según el cual, “la falta de un instrumento público no puede suplirse por otra prueba en los actos y contratos en que la ley requiere esa solemnidad”, ya que una cosa es admitir cualquier medio para probar contra lo manifestado en un documento de tal naturaleza, y otra muy distinta, sustituirlo, hipótesis a la que se refiere el artículo citado.

Veamos apartes de la sentencia de la Corte en que expone lo explicado anteriormente:

“Las declaraciones efectuadas por las partes en los instrumentos públicos pueden desvirtuarse por otro medio de prueba, puesto que, en concordancia con lo previsto en el artículo 258, ha de distinguirse, de un lado, entre el otorgamiento, la fecha y las afirmaciones del funcionario que autoriza el documento; y, del otro, las aseveraciones de los interesados, para ver cómo tan solo lo primero es lo investido con el mérito de prueba erga omnes, no excluyendo, en todo caso, la prueba que desvirtúe tales atestaciones, pues en lo que atañe con las declaraciones de las partes, si bien entre estas tienen el valor de plena prueba, tal cosa no puede ser entendida , de ninguna manera, como que no se admita prueba en contrario, o que se consideren como refutablemente sinceras y veraces, o que a los otorgantes les esté vedado infirmarlas con otros medios probatorios, ni mucho menos que se les prohíba ampararse en escritos contentivos de los acuerdos privados que permitan establecer los verdaderos designios de su voluntad”.(6)

1.1.3.4. Y continúa la Corte Suprema de Justicia: "La autenticidad de los documentos: De acuerdo con el artículo 252 del Código de Procedimiento Civil, "es auténtico un documento cuando existe certeza sobre la persona que lo ha elaborado, manuscrito o firmado. El documento público se presume auténtico, mientras que no se compruebe lo contrario mediante tacha de falsedad.

El documento privado es auténtico en los siguientes casos:

1. Si ha sido reconocido ante el juez o notario, o si judicialmente se ordenó tenerlo por reconocido.
2. Si fue inscrito en un registro público a petición de quien lo firmó.
3. Si habiéndose aportado a un proceso y afirmado estar suscrito, o haber sido manuscrito por la parte que lo suscribe, o haber sido manuscrito por la parte contra quien se opone, ésta no lo tachó de falso oportunamente, o los sucesores del causante a quien se atribuye, dejaren de hacer la manifestación contemplada en el inciso segundo del artículo 289. Esta norma se aplicará también a las reproducciones mecánicas de la voz o de la imagen de la parte contra quien se aducen, afirmándose que corresponden a ella.
4. Si fue reconocido implícitamente de conformidad con el artículo 276.

5. Si se declaró auténtico en providencia judicial dictada en proceso anterior, con audiencia de la parte contra quien se opone en el nuevo proceso, o en la diligencia de reconocimiento de que trata el artículo 274.

Se presumen auténticos los libros de comercio debidamente registrados y llevados en legal forma, el contenido y las firmas de pólizas de seguros y recibos de pago de sus primas, certificados, recibos, bonos y títulos de inversión en establecimientos de crédito y contratos de prenda con éstos, cartas de crédito, contratos de cuentas corrientes bancarias, extractos del movimiento de éstas y de cuentas con aquellos establecimientos, recibos de consignación y comprobantes de créditos, de débitos y entrega de chequeras, emitidos por los mismos establecimientos y los títulos de acciones en sociedades comerciales y bonos emitidos por éstas, títulos valores, certificados y títulos de almacenes generales de depósito, y demás documentos privados a los cuales la ley otorgue tal presunción”.(7).

1.2. SEGÚN LA GRAFIA:

La grafía de un documento es la manera en que el documento se representa y exterioriza. Según CARNELUTTI, “la representación del documento puede realizarse en forma directa o indirecta”. (8)

De manera directa, es decir, sin intermediarios, mediante la estampación fidedigna de la imagen y/o del sonido, (fotografía, cinematografía, fonografía).

De manera indirecta a través de la escritura.(9). La grafía indirecta puede realizarse de manera manual o mecánica.

1.3. **SEGÚN LA MATERIA:**

Para Luis Muñoz Sabaté, lo que se quiere aludir en el presente capítulo es a “la materia del documento, su soporte físico, del cual caben múltiples especies, ya que junto a los tipos convencionales, como el papiro, la cera, el pergamino y el papel, se dan a veces otros menos usuales, como la piedra, la corteza de un árbol, un trozo de trapo, etc. “...

...”Por otro lado, es preciso referir el concepto de materia al procedimiento mecánico empleado para la grabación (lápiz, pluma, punzón, estilete, etc.,) y en su caso a la sustancia química empleada (la tinta, pintura, etc.).

Hoy día el medio más frecuente de escritura suele ser la obtenida mediante el bolígrafo.”(10).

1.4. **SEGÚN EL CONTENIDO:**

Según GUASP, “cuando el documento crea, modifica o extingue una situación con relevancia jurídica, tendremos un documento constitutivo o dispositivo; si únicamente fija o constata la situación el documento será declarativo, y si no hace más que transcribir materialmente otro documento anterior, entonces tendremos la copia.(11).

A medida que pasa el tiempo y el hombre va trazando el camino de su historia, surgen diversas ideas e inventos útiles a él, inventos que a su vez tienden a hacerle la vida más sencilla. En esta evolución, marcada por los adelantos tecnológicos que no dejan de sorprendernos día a día, deben observarse no sólo ciertas reglas de carácter social y cultural, sino que la misma tecnología debe

impulsar el cambio que ayude a ciertas instituciones a acoplarse a lo nuevo, a lo moderno. A todo lo anterior, el derecho no puede ser indiferente, menos aún si es concebido como una ciencia social. Si los tiempos cambian y con ellos la sociedad, la cultura, las costumbres y todo lo cotidiano al hombre, es obvio que el derecho debe adaptarse a estos nuevos tiempos.

Establecida una clasificación de los documentos nos parece imprescindible adentrarnos de lleno en el estudio de la Ley 527/99 o Ley de Comercio Electrónico, que no es sino la respuesta que el legislador da a la evolución y al desarrollo tecnológico innegable e indomable que guía la vida en la sociedad actual.

La ley de Comercio Electrónico o Ley 527 de 1.999, fue expedida el 18 de Agosto de 1.999. Es una ley que consta de tres partes: una parte general, una parte dedicada al Comercio electrónico en materia de transporte de mercancías, y una parte dedicada a las firmas digitales, certificados y entidades de certificación.

En su parte general, la Ley 527 de 1.999, trata acerca de disposiciones generales y define básicamente su ámbito de aplicación, define los términos de más común utilización, fija reglas claras para su interpretación, brinda posibilidad para que las

partes mediante acuerdo, modifiquen las disposiciones relativas a la formación y validez de los contratos y, por último reconoce jurídicamente los mensajes de datos.

Por su importancia, en materia probatoria, nos parece importante analizar detalladamente la primera parte de la tabla de contenido de la ley de comercio electrónico o ley 527 de 1.999.

2. DISPOSICIONES GENERALES:

2.1. **Ambito de Aplicación:** La ley de comercio electrónico se aplica a todo tipo de información que tenga la forma de un mensaje de datos salvo en los casos de obligaciones que haya contraído el estado colombiano en virtud de tratados internacionales y en los casos de advertencias escritas que por disposición legal deban ir impresas en productos en razón al riesgo que implica su comercialización uso o consumo. Es natural que la ley de comercio electrónico haga estas distinciones en cuanto a su ámbito de aplicación ya que cierra el camino a la posible violación de normas de orden público, cuales son los tratados internacionales y las normas de

protección al consumidor, consumo, uso y comercialización de bienes y servicios.

2.2. **Definiciones:** La ley de comercio electrónico, en un importante esfuerzo por evitar falsas interpretaciones, define exactamente todo lo que se relaciona con el comercio electrónico. Así pues define lo siguiente:

2.2.1. Mensaje de datos: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos. Los medios electrónicos son el intercambio electrónico de datos, el internet, el correo electrónico, el telegrama, el télex o el telefax.

2.2.2. Comercio electrónico: el comercio electrónico está compuesto por toda relación de índole comercial, contractual o no, que se estructure a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Estas relaciones de índole comercial, son entre otras; toda operación comercial de suministro de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles o 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 de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

2.2.3. Firma digital: Se entiende como un valor numérico que adherido a un mensaje de datos y 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 original no ha sido modificado después de efectuada la transformación. Es importantísima esta definición pues a nuestro modo de ver es la columna vertebral de todo el sistema de comercio electrónico, como generador de derechos y obligaciones. Es un valor numérico, adherido a un mensaje de datos, que partiendo de la clave del iniciador, determina que ha partido de él y que no ha sido modificado.

2.2.4. Entidad de certificación: Es la persona que autorizada por la ley está facultada para emitir certificados relacionados con las firmas digitales de las personas y ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos.

- 2.2.5. Intercambio electrónico de datos: (EDI): Es la transmisión electrónica de datos de una computadora a otra, estructurada bajo normas técnicas convenidas.
- 2.2.6. Sistema de información: Se entiende como todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.
- 2.3. **Interpretación:** En la interpretación de la ley de comercio electrónico debe tenerse en cuenta que, el origen de la misma es internacional, que debe promoverse la uniformidad de su aplicación, y que debe primar la observancia de la buena fe.
- 2.4. **Modificación mediante acuerdo:** Salvo que la ley disponga otra cosa, las partes pueden modificar mediante acuerdo las disposiciones contenidas en relación con la oferta y su aceptación y la formación del contrato a partir de un mensaje de datos. Solo si media acuerdo expreso entre las partes, la oferta y su aceptación, expresadas por medio de un mensaje de datos, pueden no ser generadoras de derechos y obligaciones. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse

utilizado en su formación uno o más mensajes de datos. Este artículo adecua nuestra legislación a la rapidez del mundo moderno, otorgando fuerza vinculante a los mensajes de datos como creadores de contratos, derechos y obligaciones, exceptuando aquellos en donde haya acuerdo expreso acerca de que no son fuente generadora de las mismas.

- 2.5. **Reconocimiento jurídico de los mensajes de datos:** Piedra angular de toda la ley de comercio electrónico. En ningún momento se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté en forma de mensaje de datos. Es el reconocimiento formal y jurídico del mensaje de datos como generador de derechos y obligaciones.

Cómo aplicar los requisitos jurídicos de cualquier documento a un mensaje de datos? Es precisamente acerca de esto de lo que trata la Ley de Comercio Electrónico en su capítulo siguiente; la aplicación de los requisitos que debe cumplir cualquier documento, a los mensajes de datos, para que estos cumplan con la función generadora de derechos y obligaciones.

2.6 **Escrito:** Cuando las normas requieran que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos , si la información que el mensaje de datos contiene es accesible para su posterior consulta. De igual manera, se aplicará cuando las normas de derecho positivo prevean consecuencias en el caso que la obligación no conste por escrito. Es lógico y entendible, que la norma consagrada en el presente artículo, así como otorga validez como escrito a un mensaje de datos únicamente si la información en él contenida es accesible para su posterior consulta, le otorgue consecuencias en el caso que las normas exijan que la información conste por escrito.

2.7 **Firma:** Cuando alguna norma exija la presencia de una firma o establezca las consecuencias de la ausencia de ella, en relación con un mensaje de datos, ese requerimiento quedará satisfecho si:

2.7.1. Si se ha utilizado un método que permita identificar al iniciador del mensaje de datos y para indicar que su contenido cuenta con su aprobación y,

2.7.2. Que el método sea confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado.

2.8. **Original:** Cuando alguna norma prevea que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos si:

2.8.1. 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 datos y,

2.8.2. De necesitarse que la información sea presentada, si esa información puede ser mostrada a la persona que se deba presentar.

Al igual que en los artículos precedentes, la ley de Comercio electrónico dispone que este requisito se aplica si la norma exige la originalidad del documento al igual que si las normas simplemente prevén consecuencias en el caso que la información no sea presentada o conservada en su forma original.

2.9 **Integridad de un mensaje de datos:** La norma prevé, que la información consignada en un mensaje de datos es íntegra si ha permanecido completa e inalterada , salvo la adición de algún endoso o de algún cambio inherente al proceso de comunicación, archivo o presentación. En cuanto al grado de confiabilidad, éste se determinará de acuerdo con los fines para los cuales la información fue generada y de todas las circunstancias relevantes del caso.

2.10 Admisibilidad y fuerza probatoria de los mensajes de datos: Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada a los documentos en las disposiciones contenidas en el Capítulo VIII del Título XIII, sección tercera, libro segundo del Código de Procedimiento Civil.

Igualmente, obliga a jueces y funcionarios del orden administrativo a no negar eficacia, validez o fuerza obligatoria a todo tipo de información en forma de mensaje de datos, por el solo hecho de que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

2.11 Criterio para valorar probatoriamente un mensaje de datos: Para la valoración probatoria de un mensaje de datos, se deben tener en cuenta las reglas de la sana crítica y los demás criterios reconocidos legalmente para la apreciación de las pruebas. Por lo anterior, deben tenerse en cuenta:

2.11.1 La confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje de datos,

2.11.2 La confiabilidad en la forma en que se haya conservado la integridad de la información.

2.11.3 La forma en que se identifique a su iniciador y,

2.11.4 Cualquier otro factor pertinente.

2.12 Conservación de los mensajes de datos y documentos: En el caso de los mensajes de datos, cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, el requisito quedará satisfecho si se cumplen las siguientes condiciones:

2.12.1 Que la información contenida sea accesible para su posterior consulta.

2.12.2 Que el mensaje de datos o el documento sea conservado en el formato que se haya generado, enviado o recibido, o en algún formato que permita demostrar que reproduce la información generada, enviada o recibida.

2.12.3 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.

2.12.4 No debe conservarse la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

2.12.5 Los libros y papeles del comerciante pueden conservarse en cualquier medio técnico que garantice su reproducción exacta. (v.g. Diskettes, archivo electrónico, etc.).

2.13 **Conservación mensajes de datos y archivo de documentos a través de terceros:** El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se puede realizar

directamente o a través de terceros, siempre y cuando se cumplan las condiciones contenidas en el artículo relativo a la conservación de los mismos.

Una vez definidos por la Ley de Comercio Electrónico, la forma de los requisitos jurídicos de los mensajes de datos, ésta define de manera exacta cómo se debe producir la comunicación de los mensajes de datos.

3.1. Formación y validez de los contratos: Como ya habíamos mencionado, en la formación de los contratos, salvo un acuerdo expreso entre las partes, la oferta y su aceptación pueden ser expresadas mediante un mensaje de datos. Es el pleno reconocimiento jurídico a la eficacia del mensaje de datos para generar derechos y obligaciones. Es el reconocimiento de la legislación colombiana a un mundo en el cual la velocidad y la agilidad en la formación del acuerdo de voluntad es importantísimo y el reconocimiento de la importancia que hoy en día tienen las rápidas comunicaciones que nos gobiernan.

3.2 Reconocimiento de los mensajes de datos por las partes: En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no

pueden negarse efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad por la sola razón de haberse hecho en forma de mensaje de datos.

3.3 Atribución de un mensaje de datos: Se entiende que este proviene del iniciador cuando ha sido enviado por:

3.3.1 El propio iniciador.

3.3.2 Por alguna persona facultada por él respecto de ese mensaje y,

3.3.3 Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

3.4 Presunción del origen de un mensaje de datos: Se presume que un mensaje de datos ha sido enviado por el iniciador cuando:

3.4.1 Se haya aplicado el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía de éste o,

3.4.2 Cuando el mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como suyo.

Es importante recalcar que para que se presuma que el mensaje de datos proviene del iniciador, debe existir un procedimiento previamente acordado

para la transmisión del mensaje de datos, sin importar si lo ha transmitido directamente el iniciador, un subordinado suyo o un mandatario.

3.5 Concordancia del mensaje de datos enviado con el mensaje de datos

recibido: En las relaciones entre iniciador y destinatario, cuando el mensaje proviene del iniciador o cuando se entiende que proviene de él, o cuando el destinatario tiene derecho a suponer que proviene de él, éste último tiene derecho a suponer que el mensaje de datos corresponde al que quería enviar el iniciador y así proceder en consecuencia. El destinatario pierde ese derecho, cuando de haber actuado con la debida diligencia o al haber aplicado el método convenido, que la transmisión haya dado lugar a un error en el mensaje de datos.

3.6 Mensajes de datos duplicados:

Se presume que cada mensaje de datos es un mensaje diferente, salvo en la medida en que se duplique y, que el destinatario sepa o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el nuevo mensaje de datos era un duplicado.

3.7 Acuse de recibo:

Si al enviar o tratar de enviar un mensaje de datos , el iniciador solicita o acuerda con el destinatario que acuse recibo del mensaje

pero, no se ha acordado entre éstos un método determinado para hacerlo podrá efectuar acuse de recibo mediante:

3.7.1 Toda comunicación del destinatario automatizada o no, o

3.7.2 Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Si el iniciador ha solicitado o indicado que se requiere que se acuse recibo del mensaje de datos, y se ha indicado expresamente que los efectos del mensaje de datos están condicionados a la recepción de un acuse de recibo, se considera que el mensaje no ha sido enviado hasta tanto no se recepcione el acuse de recibo.

3.8 **Efectos jurídicos:** Los artículos precedentes sólo rigen los efectos relacionados con el acuse de recibo Las consecuencias jurídicas del mensaje de datos se rigen conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

Una vez atribuidos todos los efectos jurídicos, definiciones, creación de derechos y obligaciones de los mensajes de datos, la Ley de Comercio Electrónico se ocupa de legislar específicamente de los mensajes de datos en materia del transporte de mercancías y de las firmas digitales, las entidades de certificación y del papel que en el desarrollo de toda esta nueva legislación debe desempeñar la

Superintendencia de Industria y Comercio. Nos parece pertinente mencionar algunas cosas importantes relacionadas con el transporte de mercancías, para después adentrarnos en lo relativo con las entidades de certificación, las firmas digitales, el papel de la Superintendencia, para de esa manera, analizar y estudiar cuidadosamente las normas contenidas en el Decreto 1747 de 2.000, decreto que reglamenta las entidades de certificación, las firmas digitales, los certificados digitales y las facultades conferidas mediante éste decreto a la Superintendencia de Industria y Comercio.

4 Comercio Electrónico en materia de transporte de mercancías.

4.1 Actos relacionados con los contratos de transporte de mercancías: El presente capítulo se aplica a cualquiera de los siguientes actos que guardan relación con un contrato de transporte, o con su cumplimiento, sin que la lista sea taxativa:

4.1.1 Indicación de las marcas, el número, la cantidad o el peso de las mercancías.

4.1.2 Declaración de la naturaleza o valor de las mercancías.

4.1.3 Emisión de un recibo por las mercancías.

4.1.4 Confirmación de haberse completado el embarque de las mercancías.

4.1.5 Notificación a alguna persona de las cláusulas y condiciones del contrato.

- 4.1.6 Comunicación de instrucciones al transportador.
 - 4.1.7 Reclamación de la entrega de las mercancías.
 - 4.1.8 Notificación de la pérdida de las mercancías o de los daños que hayan sufrido.
 - 4.1.9 Cualquier otra notificación o declaración relativas al cumplimiento del contrato.
 - 4.1.10 Promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega.
 - 4.1.11 Concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías y,
 - 4.1.12 Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.
- 4.2 **Documentos de transporte:** Con sujeción a la ley de comercio electrónico, en relación con los casos en que la ley requiera la existencia de un documento emitido en papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo mediante la utilización de un mensaje de datos, mensaje de datos que debe reunir todos los requisitos establecidos en la misma ley para generar derechos y obligaciones. Es importante recalcar, que los mensajes de datos sustituyen con la misma fuerza a los escritos

emitidos en papel común y corriente, y, que previos los requisitos señalados en la ley, lo sustituyen en forma total y absoluta, hasta el momento de llegar a sustituirlo por completo y desecharlo en el caso que entre las partes se haya convenido la utilización de mensajes de datos. Es más, en el caso que un contrato de transporte conste por escrito, las normas relativas al mismo no dejarán de aplicarse si dicho contrato de mercancías conste en uno o más mensajes de datos, por el sólo hecho de no constar en documentos emitidos en papel.

5 Firmas digitales, certificados y entidades de certificación.

5.1 Firmas Digitales:

5.1.1 Atributos jurídicos de una firma digital: Cuando una firma digital se fija a un mensaje de datos, se presume que el suscriptor tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

5.1.2 El uso de una firma digital tiene la misma fuerza y efectos que el uso de una fuerza manuscrita, si la digital incorpora los siguientes atributos:

5.1.2.1 Es única a la persona que la usa.

5.1.2.2 Es susceptible de ser verificada.

- 5.1.2.3 Está bajo el control exclusivo de la persona que la usa.
- 5.1.2.4 Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
- 5.1.2.5 Está conforme a las reglamentaciones adoptadas por el gobierno nacional.

5.2 Entidades de certificación:

- 5.2.1 Características y requerimientos de las entidades de certificación: Las entidades de certificación pueden ser personas jurídicas, públicas o privadas, nacionales o extranjeras y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el gobierno nacional, con base en las siguientes condiciones:
 - 5.2.1.1 Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación.
 - 5.2.1.2 Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en la ley y,

- 5.2.1.3 Los representantes legales y administradores no pueden ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos, o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética, o hayan sido excluidas de aquella. La inhabilidad estará vigente por el mismo tiempo que la ley penal o administrativa señale para el efecto.
- 5.2.2 Las entidades de certificación autorizadas para prestar sus servicios pueden realizar entre otras, las siguientes actividades:
- 5.2.2.1 Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.
- 5.2.2.2 Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.
- 5.2.2.3 Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a la concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías y adquisición o transferencia de derechos y obligaciones con arreglo al contrato de transporte de mercancías.
- 5.2.2.4 Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.

- 5.2.2.5 Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.
 - 5.2.2.6 Ofrecer los servicios de archivo y conservación de mensajes de datos.
- 5.2.3 Deberes de las entidades de certificación: Las entidades de certificación tienen entre otros los siguientes deberes:
- 5.2.3.1 Emitir certificados conforme a lo solicitado o acordado con el suscriptor.
 - 5.2.3.2 Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos.
 - 5.2.3.3 Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.
 - 5.2.3.4 Garantizar la prestación permanente del servicio de entidad de certificación.
 - 5.2.3.5 Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores.
 - 5.2.3.6 Suministrar la información que le requieran las entidades administrativas competentes o judiciales respecto de las firmas digitales y certificados emitidos y, en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración.

- 5.2.3.7 Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio.
- 5.2.3.8 Elaborar los reglamentos que definan las relaciones con el suscriptor y la forma de prestación del servicio.
- 5.2.3.9 Llevar un registro de los certificados.

5.3 **Certificados.**

- 5.3.1 Contenido de los certificados: Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por los menos lo siguiente:
 - 5.3.1.1 Nombre, dirección y domicilio del suscriptor.
 - 5.3.1.2 Identificación del suscriptor nombrado en el certificado.
 - 5.3.1.3 El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
 - 5.3.1.4 La clave pública del usuario.
 - 5.3.1.5 La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
 - 5.3.1.6 El número de serie del certificado.
 - 5.3.1.7 Fecha de emisión y expiración del certificado.

5.3.2 Aceptación de un certificado: Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio.

5.3.3 Revocación de Certificados.

5.3.3.1 El suscriptor de una firma digital certificada, puede solicitar a la entidad de certificación, que expidió un certificado, la revocación del mismo. Está obligado a solicitar la revocación en los siguientes eventos y, si no lo hace, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exente de culpa, que confiaron en el contenido del certificado. Estos eventos son:

5.3.3.1.1 Por pérdida de la clave privada.

5.3.3.1.2 La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

5.3.3.2 La entidad de certificación revocará un certificado emitido por las siguientes razones:

5.3.3.2.1 A petición del suscriptor o un tercero en su nombre y representación.

5.3.3.2.2 Por muerte del suscriptor.

5.3.3.2.3 Por liquidación del suscriptor en el caso de las personas jurídicas.

- 5.3.3.2.4 Por la confirmación de que alguna información o hecho contenido en el certificado es falso.
- 5.3.3.2.5 La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.
- 5.3.3.2.6 Por el cese de actividades de la entidad de certificación.
- 5.3.3.2.7 Por orden judicial o de entidad administrativa competente.
- 5.3.3.3 Término de conservación de los registros: Los registros de certificados deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular.

5.4 Suscriptores de firmas digitales.

- 5.4.1 Deberes de los suscriptores: Son deberes de los suscriptores:
 - 5.4.1.1 Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.
 - 5.4.1.2 Suministrar la información que requiera la entidad de certificación.
 - 5.4.1.3 Mantener el control de la firma digital.
 - 5.4.1.4 Solicitar oportunamente la revocación de los certificados.

5.4.2 Responsabilidad de los suscriptores. Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.

6 Superintendencia de Industria y Comercio.

6.1 **Funciones de la Superintendencia de Industria y Comercio:** La Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación y adicionalmente las siguientes:

6.1.1 Autorizar la actividad de la entidades de certificación en el territorio nacional.

6.1.2 Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación.

6.1.3 Realizar visitas de auditoría a las entidades de certificación.

6.1.4 Revocar o suspender la autorización para operar como entidad de certificación.

6.1.5 Solicitar la información pertinente para el ejercicio de sus funciones.

- 6.1.6 Imponer sanciones a las entidades de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.
 - 6.1.7 Ordenar la revocación de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.
 - 6.1.8 Designar los repositorios y entidades de certificación en los eventos previstos en la ley.
 - 6.1.9 Emitir certificados en relación con las firmas digitales de las entidades de certificación.
 - 6.1.10 Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación.
 - 6.1.11 Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.
- 6.2 **Sanciones:** La Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer, las siguientes sanciones a las entidades de certificación:
- 6.2.1 Amonestación.

- 6.2.2 Multas institucionales hasta por el equivalente a dos mil (2.000) salarios mínimos legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades de certificación, hasta por trescientos (300) salarios mínimos legales mensuales vigentes, cuando se les compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.
- 6.2.3 Suspender de inmediato todas o algunas de las actividades de la entidad infractora.
- 6.2.4 Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.
- 6.2.5 Revocar definitivamente la autorización para operar como entidad de certificación.

Para garantizar la internacionalidad de la Ley de Comercio electrónico, y el reconocimiento de la globalización de los mensajes de datos, las firmas digitales y el comercio electrónico, el gobierno nacional, previó disposiciones varias, que garantizarán el carácter internacional del comercio electrónico. Estas disposiciones son las siguientes:

7 Disposiciones Varias.

- 7.1 Certificaciones recíprocas:** Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados , la regularidad de los detalles del certificado, así como su validez y vigencia.
- 7.2 Incorporación por remisión:** Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a ese mensaje de datos. Entre las partes, conforme a la ley, esos términos serán jurídicamente válidos, como si hubieran sido incorporados en su totalidad en el mensaje de datos.

En Septiembre 11 de 2.000, el presidente de la República en uso de sus facultades legales, expidió el Decreto número 1747, por medio del cual reglamenta parcialmente la Ley 527 de 1.999 o Ley de Comercio Electrónico, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

8 Decreto Número 1747 de 2.000.

8.1 Aspectos Generales.

8.1.1 Definiciones: El decreto 1747 de 2.000 trae las siguientes definiciones las cuales, por su importancia creemos deben ser analizadas y mencionadas en su totalidad.

8.1.1.1 Iniciador: Es la persona que actuando por su cuenta, o en cuyo nombre se haya actuado, envíe o genere un mensaje de datos.

8.1.1.2 Suscriptor: Es la persona a cuyo nombre se expide un certificado.

8.1.1.3 Repositorio: sistema de información utilizado para almacenar y recuperar certificados y otra información relacionada con los mismos.

8.1.1.4 Clave Privada: valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

- 8.1.1.5 Clave pública: valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador.
- 8.1.1.6 Certificado en relación con las firmas digitales: mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la clave pública de éste.
- 8.1.1.7 Estampado cronológico: mensaje de datos firmado por una entidad de certificación que sirve para verificar que otro mensaje de datos no ha cambiado en un período que comienza en la fecha y hora en que se presta el servicio y termina en la fecha en que la firma del mensaje de datos generado por el prestador del servicio de estampado, pierde validez.
- 8.1.1.8 Entidad de certificación cerrada: 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.
- 8.1.1.9 Entidad de certificación abierta: la que ofrece servicios propios de las entidades de certificación, tales que:
 - 8.1.1.9.1 Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o
 - 8.1.1.9.2 Recibe remuneración por éstos.

8.1.1.10 Declaración de prácticas de certificación, DPC: manifestación de la entidad de certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.

8.2 De las entidades de certificación y certificados digitales.

8.2.1 De las entidades de certificación cerradas.

8.2.1.1 Los requisitos que deben acreditar quienes pretendan realizar las actividades propias de las entidades de certificación cerradas ante la Superintendencia de Industria y Comercio son:

8.2.1.1.1 Que los administradores y representantes legales no están incurso en las causales de inhabilidad previstas en el literal c) del artículo 29 de la ley 527 de 1.999.

8.2.1.1.2 Que están en capacidad de cumplir los estándares mínimos que fije la Superintendencia de Industria de Comercio de acuerdo a los servicios ofrecidos.

8.2.1.2 Los certificados emitidos por las entidades de certificación cerradas deben indicar expresamente que sólo pueden ser utilizados entre la entidad emisora y el suscriptor. Estas entidades tienen la obligación de informar al suscriptor, de manera clara y expresa, previa expedición del

certificado que éste no cumple los requisitos establecidos en el artículo 15 del decreto 1747 de 2.000.

8.2.2 De las entidades de certificación abiertas.

8.2.2.1 Los requisitos que deben acreditar ante la Superintendencia de Industria y Comercio, las entidades que pretendan realizar las actividades de certificación abiertas son:

8.2.2.1.1 Personería jurídica o condición de notario o cónsul. Cuando se trate de una entidad extranjera, debe acreditar el cumplimiento de los requisitos establecidos en el libro segundo, título VIII del Código de Comercio, es decir, todo lo relativo al establecimiento y operación de las sociedades extranjeras en Colombia. Al igual que lo contemplado en el artículo 48 del Código de Procedimiento Civil.

8.2.2.1.2 Que los administradores y representantes legales no estén incurso en las inhabilidades previstas en el artículo 29 de la ley 527 de 1.999.

8.2.2.1.3 Declaración de prácticas de certificación, DPC, satisfactoria, de acuerdo con los requisitos establecidos por la Superintendencia de Industria y Comercio.

8.2.2.1.4 Patrimonio mínimo de 400 salarios mínimos mensuales legales vigentes al momento de la autorización.

- 8.2.2.1.5 Constitución de las garantías previstas en este decreto.
 - 8.2.2.1.6 Infraestructura y recursos por lo menos en la forma exigida en el artículo 9° de este decreto.
 - 8.2.2.1.7 Informe inicial de auditoría satisfactorio a juicio de la misma Superintendencia.
 - 8.2.2.1.8 Un mecanismo de ejecución inmediata para revocar los certificados digitales expedidos a los suscriptores, a petición de estos o cuando se tenga indicios de que ha ocurrido alguno de los eventos previstos en el artículo 37 de la Ley 527 de 1.999.
 - 8.2.2.1.9 La Superintendencia tiene la facultad de solicitar ampliación o aclaración sobre los puntos que estime conveniente y,
 - 8.2.2.1.10 Si la entidad solicita autorización para certificaciones recíprocas, se deben acreditar igualmente la entidad reconocida, los certificados reconocidos y el tipo de certificados al cual se remite, la vigencia y los términos del reconocimiento.
- 8.2.2.2 Declaración de Prácticas de Certificación, DPC: A la Superintendencia de Industria y Comercio le corresponde definir el contenido de la declaración de prácticas de certificación, DPC, la que debe incluir al menos lo siguiente:

- 8.2.2.2.1 Identificación de la entidad de Certificación.
- 8.2.2.2.2 Política de manejo de los certificados.
- 8.2.2.2.3 Obligaciones de la entidad y de los suscriptores del certificado y precauciones que deben observar los terceros.
- 8.2.2.2.4 Manejo de la información suministrada por los suscriptores.
- 8.2.2.2.5 Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.
- 8.2.2.2.6 Límites de responsabilidad para el ejercicio de su actividad.
- 8.2.2.2.7 Tarifas de expedición y revocación de certificados.
- 8.2.2.2.8 Procedimientos de seguridad para el manejo de los siguientes eventos:
 - 8.2.2.2.8.1 Cuando la seguridad de la clave privada de la entidad de certificación se ha visto comprometida.
 - 8.2.2.2.8.2 Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
 - 8.2.2.2.8.3 Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.
 - 8.2.2.2.8.4 Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratados por el suscriptor.
- 8.2.2.2.9 El plan de contingencia encaminado a garantizar la continuidad del servicio de certificación.

- 8.2.2.2.10 Modelos y minutas de los contratos que utilizarán con los usuarios.
- 8.2.2.2.11 Política de manejo de otros servicios que fuere a prestar, detallando sus condiciones.
- 8.2.2.3 Patrimonio mínimo: Para determinarlo 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:
- 8.2.2.3.1 En el caso de personas jurídicas por medio de estados financieros, con una antigüedad no superior a seis meses, certificados por el representante legal y el revisor fiscal si lo hubiere.
- 8.2.2.3.2 En el caso de entidades públicas por medio del proyecto de gastos e inversión que generará la actividad de certificación, junto con los certificados de disponibilidad presupuestal que acrediten la apropiación de recursos para tal fin.
- 8.2.2.3.3 Para las sucursales de entidades extranjeras, por medio del capital asignado.
- 8.2.2.3.4 En el caso de notarios y cónsules, por medio de los recursos dedicados exclusivamente a la actividad de entidad de certificación.

8.2.2.4 Garantías. La entidad debe contar con al menos una de las siguientes garantías:

8.2.2.4.1 Seguros vigentes que cumplan con los siguientes requisitos:

8.2.2.4.1.1 Ser expedidos por una entidad aseguradora autorizada para operar en Colombia, o por una entidad aseguradora del exterior que cuente con la autorización previa de la Superintendencia Bancaria.

8.2.2.4.1.2 Cubrir todos los perjuicios contractuales o extracontractuales de los suscriptores y terceros de buena fe exenta de culpa, derivados de errores u omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la certificadora en el desarrollo de sus actividades.

8.2.2.4.1.3 Cubrir los anteriores riesgos por una cuantía asegurada por evento igual o superior al mayor entre:

8.2.2.4.1.3.1 7.500 salarios mínimos mensuales legales por evento; o

8.2.2.4.1.3.2 El límite de responsabilidad definido en las prácticas de certificación.

8.2.2.4.1.4 Incluir cláusula de restitución automática del valor asegurado, y

8.2.2.4.1.5 Incluir una cláusula que obligue a la entidad aseguradora a informar previamente a la Superintendencia de Industria y Comercio la

terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.

8.2.2.4.2 Contrato de Fiducia con patrimonio autónomo que cumpla con las siguientes características:

8.2.2.4.2.1 Tener como objeto exclusivo el cubrimiento de las pérdidas sufridas por los suscriptores y terceros de buena fe exentos de culpa, que se deriven de los errores y omisiones o de actos de mala fe de los administradores, representantes legales o empleados de la certificadora en el desarrollo de las actividades.

8.2.2.4.2.2 Contar con recursos suficientes para cubrir pérdidas por una cuantía por evento igual o superior al mayor entre:

8.2.2.4.2.2.1 7.500 salarios mínimos mensuales legales por evento; o

8.2.2.4.2.2.2 El límite de responsabilidad definido en las prácticas de certificación.

8.2.2.4.2.3 Que los fideicomitentes se obliguen a restituir los recursos de la fiducia en caso de una reclamación, por lo menos hasta el monto mínimo exigido en el punto anterior.

8.2.2.4.2.4 Que la fiduciaria se obligue a obtener permiso de la Superintendencia de Industria y Comercio, previamente a cualquier cambio en los reglamentos, disminución en el monto o alcance de la

cobertura, así como para el retiro de fideicomitentes y para la terminación del contrato.

8.2.2.4.2.5 Que las inversiones estén representadas en títulos de renta fija, alta seguridad y liquidez emitidos o garantizados por la nación, el Banco de la República o calificados como de mínimo riesgo por las sociedades calificadoras de riesgo.

8.2.2.5 Infraestructura y recursos: La entidad debe contar con un equipo de personas, una infraestructura física y tecnológica y unos procedimientos y sistemas de seguridad, tales que:

8.2.2.5.1 Puedan generar las firmas digitales propias y todos los servicios para los que soliciten autorización.

8.2.2.5.2 Se garantice el cumplimiento de lo previsto en la declaración de prácticas de certificación, DPC.

8.2.2.5.3 Se pueda calificar el sistema como confiable, es decir, si satisfacen los estándares establecidos por la Superintendencia de Industria y Comercio.

8.2.2.5.4 Los certificados expedidos por las entidades cumplan con:

8.2.2.5.4.1 El mínimo contenido establecido por la ley 527 de 1.999 para los certificados emitidos por una entidad de certificación autorizada.

- 8.2.2.5.4.2 Alguno de los estándares de certificados que admita la Superintendencia de Industria y Comercio.
- 8.2.2.5.5 Se garantice la existencia de sistemas de seguridad física en sus instalaciones, un monitoreo permanente de toda su planta física, y acceso restringido a los equipos que manejan los sistemas de operación de la entidad.
- 8.2.2.5.6 El manejo de la clave privada de la entidad esté sometido a un procedimiento de seguridad que evite el acceso físico o de otra índole a la misma.
- 8.2.2.5.7 Cuento con un registro de todas las transacciones realizadas, que permita identificar el autor de cada una de las operaciones.
- 8.2.2.5.8 Los sistemas que cumplan las funciones de certificación sólo sean utilizados con ese propósito y por lo tanto no pueden realizar ninguna otra función.
- 8.2.2.5.9 Todos los sistemas que participen directa o indirectamente en la función de certificación estén protegidos por sistemas y procedimientos de autenticación y seguridad de alto nivel de protección, los cuales deben ser permanentemente actualizados.

- 8.2.2.6 Infraestructura prestada por un tercero: Cuando la entidad utilice infraestructura o servicios tecnológicos prestados por un tercero, los contratos deben prever que su terminación está condicionado a que la entidad haya implementado o contratado una infraestructura o servicio tecnológico que le permita seguir prestando el servicio sin ningún perjuicio para los suscriptores. Es obvio que la contratación de esta infraestructura no exime a la entidad de la presentación de los informes de auditoría, los cuales deben incluir los sistemas y seguridades de dicho prestador.
- 8.2.2.7 Informe de Auditoría. El informe de auditoría dictaminará que la entidad de certificación actúa o está en capacidad de actuar con los requerimientos de la Ley 527 de 1.999 y demás legislación complementaria y reglamentaria. Así mismo evaluará todos los servicios que preste o pretenda prestar la entidad certificadora.
- 8.2.2.8 Requisitos de las firmas auditoras. La auditoría debe realizarla una entidad del sistema nacional de normalización, certificación y metrología acreditada para el efecto por la Superintendencia de Industria y Comercio. Si la entidad certificadora requiere o utilice infraestructura o servicios tecnológicos prestados en el exterior, la auditoría puede hacerse en el lugar donde se encuentre la infraestructura, siempre y

cuando pueda constatarse el cumplimiento de lo señalado anteriormente.

8.2.2.9 Deberes: Además de lo previsto en la Ley 527 de 1.999, las entidades de certificación deberán:

8.2.2.9.1 Comprobar por sí o por medio de una persona diferente, que actúe en nombre y por cuenta suya, comprobar la identidad y cualesquiera otras circunstancias de los solicitantes o de datos de los certificados para los fines propios de su procedimiento de verificación previo a su expedición.

8.2.2.9.2 Mantener a disposición permanente del público la declaración de prácticas de certificación.

8.2.2.9.3 Cumplir cabalmente con las políticas de certificación acordadas con el suscriptor y con su declaración de prácticas de certificación.

8.2.2.9.4 Informar al suscriptor de los certificados que expide, su nivel de confiabilidad, los límites de responsabilidad y las obligaciones que el suscriptor asume como usuario del servicio de certificación.

8.2.2.9.5 Garantizar la prestación permanente e ininterrumpida de los servicios autorizados, salvo las interrupciones autorizadas por la Superintendencia de Industria y Comercio.

- 8.2.2.9.6 Informar a la superintendencia de manera inmediata de cualquier evento establecido en las prácticas de certificación, que comprometa la prestación del servicio.
- 8.2.2.9.7 Abstenerse de acceder o almacenar la clave privada del suscriptor.
- 8.2.2.9.8 Mantener actualizado el registro de los certificados revocados. Ellos son responsables de los perjuicios que se causen a terceros por incumplimiento de ésta obligación.
- 8.2.2.9.9 Garantizar el acceso permanente y eficiente de los suscriptores y de terceros al repositorio de la entidad.
- 8.2.2.9.10 Disponer de una línea telefónica de atención permanente a suscriptores y terceros, que permita consultas y pronta solicitud de revocación de certificados por los suscriptores.
- 8.2.2.9.11 Garantizar la confidencialidad de la información que no figure en el certificado.
- 8.2.2.9.12 Conservar la documentación que respalda los certificados emitidos, por el término previsto en la ley para los papeles de los comerciantes y tomar las medidas para garantizar la integridad y confidencialidad que le son propias.
- 8.2.2.9.13 Informar al suscriptor dentro de las 24 horas siguientes, la suspensión del servicio o revocación de sus certificados.

- 8.2.2.9.14 Capacitar y advertir a los suscriptores de firmas y certificados digitales, sobre las medidas de seguridad que deben observar para la utilización de estos mecanismos.
- 8.2.2.9.15 Mantener el control exclusivo de su clave privada y establecer las seguridades necesarias para que no se divulgue o comprometa.
- 8.2.2.9.16 Remitir oportunamente a la Superintendencia de Industria y Comercio, la información prevista en este decreto.
- 8.2.2.9.17 Remover en el menor término que el procedimiento legal permita, a los administradores o representantes incursos en inhabilidades.
- 8.2.2.9.18 Informar a los suscriptores o terceros que lo soliciten, sobre el tiempo y recursos computacionales requeridos para derivar la clave privada a partir de la clave pública contenida en los certificados en relación con las firmas digitales que expide la entidad.
- 8.2.2.9.19 Mantener actualizada la información registrada en la solicitud de autorización y enviar la información que la Superintendencia de Industria y Comercio establezca.
- 8.2.2.9.20 Cumplir con las demás instrucciones que establezca la Superintendencia de Industria y Comercio.

- 8.2.2.10 **Certificaciones Recíprocas:** El reconocimiento de los certificados de firmas digitales emitidos por entidades de certificación extranjeras, realizados por entidades de certificación autorizadas en Colombia, se hará constar en un certificado expedido por estas últimas. El efecto del reconocimiento de cada certificado, se limitará a las características propias del certificado reconocido y por el período de validez del mismo. La Superintendencia de Industria y Comercio determinará el contenido mínimo de los certificados recíprocos.
- 8.2.2.11 **Uso del certificado digital.** Cuando un suscriptor firme digitalmente un mensaje de datos con su clave privada, y la respalde mediante un certificado digital, se darán por satisfechos los atributos exigidos para una firma digital en la Ley 527 de 1.999, sí:
- 8.2.2.11.1 El certificado fue emitido por una entidad de certificación abierta autorizada por la Superintendencia de Industria y Comercio.
- 8.2.2.11.2 Dicha firma se puede verificar en la clave pública que se encuentra en el certificado con relación a firmas digitales, emitido por la entidad de certificación.
- 8.2.2.11.3 La firma fue emitida dentro del tiempo de validez del certificado, sin que éste haya sido revocado.

8.2.2.11.4 El mensaje de datos firmado se encuentra dentro de los usos aceptados en la declaración de prácticas de certificación, de acuerdo al tipo de certificado.

8.2.2.12 Unicidad de la firma digital. Una firma digital en un mensaje de datos deja de ser única a la persona que la usa si, estando bajo su control exclusivo, la probabilidad de derivar la clave privada, a partir de la clave pública no es o deja de ser remota. Para establecer si la posibilidad es remota, se tendrán en cuenta la utilización del máximo recurso computacional disponible al momento de calcular la probabilidad, durante un período igual al que transcurre entre el momento en que se crean el par de claves y aquel en que el documento firmado deja de ser idóneo para generar obligaciones.

8.2.3 De la decisión y las responsabilidades.

8.2.3.1 En la resolución de autorización expedida por la Superintendencia de Industria y Comercio, se deben precisar las actividades y servicios que puede prestar la entidad de certificación. En todo caso, la entidad puede solicitar autorización para prestar actividades y servicios adicionales.

- 8.2.3.2 Responsabilidad: Las entidades de certificación responderán por todos los perjuicios que causen en el ejercicio de sus actividades.
- 8.2.3.3 Cesación de actividades: La cesación de actividades de una entidad certificadora sin autorización o la continuación de actividades después de producida la cesación, la hará responsable de todos los perjuicios que cause a sus suscriptores y a terceros y la hará acreedora a las sanciones que imponga la superintendencia.
- 8.2.3.4 Responsabilidad derivada de la administración de los repositorios: Cuando las entidades certificadoras contraten los servicios de repositorios, continuarán siendo responsables frente a sus suscriptores y terceros por el mismo.
- 8.2.3.5 Información periódica y esporádica: La información relativa a la acreditación de requisitos de las entidades de certificación cerradas, la acreditación de requisitos de las entidades de certificación abiertas, la declaración de prácticas de certificación, lo relativo al patrimonio mínimo, la información relativa a garantías, a infraestructura y recursos, a infraestructura prestada por un tercero y a los informes de auditoría, es información que debe actualizarse ante la Superintendencia de Industria y Comercio cada vez que haya cambios o modificaciones de los datos suministrados.

8.2.3.6 Responsabilidad derivada de la no revocación. Una vez cumplidas las formalidades previstas para la revocación, la entidad será responsable por los perjuicios que cause la no revocación.

8.2.4 De los certificados digitales.

8.2.4.1 Información relativa a la revocación: Cada certificado revocado debe indicar si el motivo de revocación incluye la pérdida de control de la clave privada, evento en el cual, las firmas generadas con dicha clave privada carecerán del atributo de unidad, salvo que se demuestre lo contrario, mediante un mecanismo adicional que pruebe inequívocamente que el documento fue firmado digitalmente en una fecha previa a la revocación del certificado. Las revocaciones deben ser publicadas de manera inmediata en los repositorios correspondientes y notificadas al suscriptor dentro de las 24 horas siguientes. Si dichos repositorios no existen al momento de la publicación del aviso, ésta se efectuará en un repositorio que designe la Superintendencia de Industria y Comercio.

8.2.4.2 Registro de Certificados: Toda entidad de certificación estará obligada a llevar un registro de público acceso que contenga los certificados emitidos y sus fechas de emisión, expiración o revocación.

8.2.4.3 Información. Las entidades de certificación estarán obligadas a respetar las condiciones de confidencialidad y seguridad. Salvo la información contenida en el certificado, la suministrada por los suscriptores a las entidades de certificación se considerará privada y confidencial

8.3 Facultades de la Superintendencia de Industria y Comercio.

8.3.1 Suspensión y revocación de Autorización: Cuando la Superintendencia de Industria y Comercio ejerza la facultad de revocar o suspender la autorización para operar como entidad de certificación, ordenará a la entidad de certificación la ejecución de medidas tendientes a garantizar la integridad, seguridad y conservación de los certificados expedidos, así como la compensación económica que pudiera generar la cesación de actividades.

8.3.2 Estándares: La Superintendencia de Industria y Comercio determinará los estándares admisibles con respecto a los cuales, las entidades de certificación deberán acreditar el cumplimiento de los requisitos relativos a:

8.3.2.1 La generación de pares de claves.

8.3.2.2 La generación de firmas.

8.3.2.3 Los certificados.

8.3.2.4 Los sistemas de cifrado.

8.3.2.5 Las comunicaciones.

8.3.2.6 La seguridad de los sistemas de información y de las instalaciones, o

8.3.2.7 Cualquier otro aspecto que redunde en la confiabilidad y seguridad de los certificados, o de la información que repose en la entidad de certificación.

Para determinar los estándares admisibles, la Superintendencia debe adoptar aquellos que tengan carácter internacional y que estén vigentes tecnológicamente o los desarrollados por el organismo nacional de normalización o los que sean ampliamente reconocidos para los propósitos perseguidos. En todo caso debe tener en cuenta su aplicabilidad a la luz de la legislación vigente. Igualmente la Superintendencia puede eliminar la admisibilidad de un estándar cuando haya dejado de cumplir alguno de los requisitos precisados.

El 26 de Octubre de 2.000, el Ministerio de Desarrollo Económico y la Superintendencia de Industria y Comercio, con base en las facultades conferidas en la ley 527 de 1.999 y en el decreto 1747 de 2.000, expide la Resolución 26930 con el objeto de fijar los requisitos para autorizar la actividad de las entidades de certificación, velar por su funcionamiento y la prestación del servicio, así como impartir las instrucciones sobre el adecuado cumplimiento de las normas a las

cuales deben sujetarse las entidades de certificación, la autorización para cesación de sus actividades y la solicitud a personas naturales o jurídicas del suministro de información, datos, informes, libros y papeles de comercio que se requieran para el correcto ejercicio de sus funciones. En virtud de lo anterior, se expidió la Resolución 26930, resolución, que en términos generales regula lo siguiente:

9. Resolución No. 26930 de Octubre 26 de 2.000

9.1 Entidades de Certificación Cerradas.

9.1.1 La persona que solicite autorización como entidad de certificación cerrada, debe demostrar el cumplimiento de las condiciones establecidas en el artículo 29 de la Ley 527 de 1.999 y en los artículos 3° y 4° del decreto 1747 de 2.000, adjuntando los siguientes documentos:

9.1.1.1 Certificado de existencia y representación legal, o copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul.

9.1.1.2 Un formato (establecido por la Superintendencia de Industria y Comercio), por cada uno de los administradores o representantes legales.

- 9.1.2 Cuando la entidad de certificación cerrada pretenda ofrecer nuevos servicios, dentro del entorno cerrado, deberá solicitar ante la Superintendencia de Industria y Comercio.
- 9.1.3 Cuando alguno de los datos de la entidad de certificación cerrada cambie, la entidad de certificación deberá remitir la información correspondiente al cambio dentro de los 10 días posteriores a la modificación. Si se trata de modificación respecto a un administrador o a un representante legal debe incluirse el formato dispuesto por la Superintendencia.
- 9.1.4 La entidad de certificación debe almacenar la información de toda su actividad y enviar a la Superintendencia dentro de los 10 primeros días del inicio de cada trimestre un archivo de texto con la siguiente información:
- 9.1.4.1 Número de certificados emitidos, de acuerdo con el tipo de certificados.
 - 9.1.4.2 Número de certificados vigentes, de acuerdo con el tipo de certificados.
 - 9.1.4.3 Número de certificados revocados.
- 9.1.5 Las entidades de certificación cerradas deben solicitar autorización de cesación de una o más actividades ante la Superintendencia de Industria y Comercio. Una vez autorizada, debe concluir el ejercicio de las actividades

autorizadas para cesar, en la forma y siguiendo el cronograma que para tal efecto se señale.

- 9.1.6 En cualquier publicidad o en cualquier medio en el cual la entidad de certificación ofrezca los servicios debe indicar que cuenta con autorización de la Superintendencia de Industria y Comercio para operar, según el siguiente texto: “Entidad de certificación cerrada autorizada por la Superintendencia de Industria y Comercio”.

Es importante resaltar que en la actualidad sólo existe una entidad de certificación cerrada autorizada por la Superintendencia de Industria y Comercio para operar cuyo nombre es SERDINET S.A.

9.2 Entidades de Certificación Abiertas.

9.2.1 Autorización

- 9.2.1.1 La persona que solicite autorización como entidad de certificación abierta, deberá demostrar que la actividad está prevista en el objeto social principal, el cumplimiento de las condiciones establecidas en la Ley 527 de 1.999 y en el decreto 1747 de 2.000, así como los estándares, planes y procedimientos de seguridad, adjuntando la siguiente información:

- 9.2.1.1.1 Anexo debidamente diligenciado para cada uno de los administradores o representantes legales adjuntando certificado judicial vigente o documento equivalente proveniente del país o países donde haya residido y copia del certificado de representación legal o copia de las normas que le otorguen la calidad de representante legal de una entidad pública o de notario o cónsul.
- 9.2.1.1.2 Copia del acto que le otorga personería jurídica y copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul, o certificado de existencia y representación legal. Cuando se trate de persona extranjera se debe acreditar el cumplimiento de lo señalado en el libro II título XIII del código de comercio y el artículo 48 del código de procedimiento civil.
- 9.2.1.1.3 Informe de auditoría en los términos de ésta Resolución.
- 9.2.1.1.4 Estados financieros certificados conforme a la ley y con una antigüedad no superior a seis meses.
- 9.2.1.1.5 Copia del documento que acredite que han constituido las garantías.
- 9.2.1.1.6 Documento con descripción detallada de la infraestructura, procedimientos y recursos. En caso que la infraestructura sea prestada por un tercero, copia de los contratos o convenios con los terceros, en idioma español.

9.2.1.1.7 Declaración de prácticas de certificación.

9.2.2 Cumplimiento de requisitos permanentes.

9.2.2.1 Cuando la entidad de certificación abierta pretenda ofrecer nuevos servicios, debe solicitar autorización previa a la Superintendencia de Industria y Comercio, adjuntando el informe de auditoría correspondiente al nuevo servicio.

9.2.2.2 Cuando alguno de los datos de la entidad de certificación que reposan en la Superintendencia cambien, la entidad de certificación debe remitir la información correspondiente al cambio, dentro de los 10 días posteriores a la modificación. Si se trata de modificación de la información o inclusión de un representante legal o administrador, el nuevo representante legal o administrador debe diligenciar el anexo correspondiente y remitirlo adjuntando:

9.2.2.2.1 Certificado judicial vigente o documento equivalente del país o países donde haya residido.

9.2.2.2.2 Certificado del órgano competente de los países en que haya residido que certifique que no ha sido excluido o suspendido por actos graves contra la ética de la profesión.

- 9.2.2.3 La entidad de certificación abierta debe almacenar toda la información de su actividad y enviara la Superintendencia dentro de los 10 primeros días del inicio de cada trimestre un archivo de texto con la siguiente información sobre la actividad del trimestre anterior, discriminada mes a mes:
- 9.2.2.3.1 Número de certificados emitidos de acuerdo con el tipo de certificados.
 - 9.2.2.3.2 Número de certificados vigentes, de acuerdo con el tipo de certificados.
 - 9.2.2.3.3 Número de certificados revocados.
 - 9.2.2.3.4 Compromisos adquiridos por cada tipo de certificado.
- 9.2.2.4 La entidad de certificación abierta debe remitir a la Superintendencia de Industria y Comercio los estados financieros de fin de ejercicio y el informe de auditoría dentro de los primeros 15 días corrientes de Febrero de cada año calendario.
- 9.2.2.5 Durante cada año calendario, las entidades de certificación podrán cesar temporalmente sus servicios durante un lapso máximo de tres días continuos o discontinuos, para mantenimiento del sistema. Cualquier otra suspensión debe ser solicitada y aprobada por la Superintendencia de Industria y Comercio. La suspensión permitida deberá informarse a los usuarios con por lo menos 15 días de

antelación. La constancia del aviso debe remitirse a la Superintendencia a más tardar el primer día de la suspensión.

9.2.2.6 En cualquier medio en la cual la entidad de certificación ofrezca sus servicios debe indicar que cuenta con autorización de la Superintendencia para operar, según el texto siguiente: “ Entidad de certificación abierta autorizada por la Superintendencia de Industria y Comercio”.

9.2.3 Firmas auditoras de entidades de certificación.

9.2.3.1 La firma auditora nacional que realice el informe de auditoría, debe ser un organismo de inspección del sistema nacional de normalización, certificación y metrología acreditada para realizar inspecciones en sistemas informáticos de seguridad y contabilidad. Estas firmas aparte de lo establecido en el decreto 2269 de 1.993 deben cumplir lo siguiente:

9.2.3.1.1 Estar compuesta por un grupo interdisciplinario de profesionales que incluirá por lo menos 1 ingeniero especializado en sistemas de seguridad, 1 contador y 1 abogado con amplios conocimientos en el tema.

- 9.2.3.1.2 Acreditar experiencia de la firma o de uno de los socios o funcionarios, en auditorías en sistemas informáticos de seguridad y contabilidad por lo menos de 3 años.
- 9.2.3.1.3 Acreditar capacidad para certificar el cumplimiento de los requisitos técnicos y estándares exigidos en la Ley 527 de 1.999, decreto 1747 de 2.000 y Resolución 26930.
- 9.2.3.2 El informe de auditoría debe indicar por lo menos:
- 9.2.3.2.1 Nombre e identificación de la firma auditora.
- 9.2.3.2.2 Fecha de inicio y terminación de la auditoría.
- 9.2.3.2.3 Declaración de conformidad de cada una de las condiciones previstas en el artículo 29 de la Ley 527 de 1.999, el decreto 1747 de 2.000, la presente resolución y las normas que los modifiquen o adicionen.
- 9.2.3.2.4 Manifestación de conformidad de las prácticas de certificación y evaluación de la efectividad de los planes, políticas y procedimientos de seguridad contenidos en la declaración y en la sección V de la resolución 26930.
- 9.2.3.2.5 Manifestación del cumplimiento de los estándares indicados en la resolución 26930 de 2.000, teniendo en cuenta criterios reconocidos, que cumplan por lo menos con los objetivos del nivel de protección 2. En

el informe debe precisar para cada uno de los objetivos el criterio que observó, la fuente de ese criterio y el reconocimiento que tiene.

9.2.3.2.6 Firma del representante legal de la firma auditora.

9.2.4 Cesación de actividades

9.2.4.1 Las entidades de certificación abiertas deben solicitar autorización de cesación de una o más actividades ante la Superintendencia de Industria y Comercio, y adjuntando la siguiente información:

9.2.4.1.1 Plan que garantice la protección de la información confidencial de los suscriptores.

9.2.4.1.2 Plan de conservación de los archivos necesarios para futuras verificaciones de los certificados que emitió, hasta el otorgamiento de la autorización de cesación del servicio. El plan debe extenderse hasta una fecha posterior a la fecha en que se extingan las responsabilidades que se puedan derivar de los certificados expedidos y el plazo que prevean las normas de conservación documental.

9.2.4.1.3 Plan que garantice la publicación de los repositorios propios si no cesa todas las actividades o en los de otra entidad de certificación abierta que la Superintendencia de Industria y Comercio determine, si cesara todas las actividades.

9.2.4.1.4 En caso de cesar todas las actividades de entidad de certificación, un plan de seguridad que garantice la adecuada destrucción de la clave privada de la entidad.

9.2.4.2 Una vez la Superintendencia autorice la cesación de actividades, la entidad de certificación, deberá informar a todos los suscriptores, mediante dos avisos publicados en diarios de amplia circulación nacional, con un intervalo de 15 días, sobre:

9.2.4.2.1 La terminación de su actividad o actividades y la fecha precisa de cesación.

9.2.4.2.2 Las consecuencias jurídicas de la cesación respecto de los certificados expedidos.

En todo caso los suscriptores pueden solicitar la revocación y el reembolso equivalente al valor del tiempo de vigencia restante del certificado, si lo solicitan dentro de los dos meses siguientes a la segunda publicación. Es natural que la terminación de la actividad o actividades se hará en la forma y siguiendo el cronograma que para el efecto señale la Superintendencia.

9.2.5 Estándares, planes y procedimientos de seguridad.

- 9.2.5.1 Para los efectos del artículo 27 del decreto 1747 de 2.000, se admitirán los siguientes estándares:
- 9.2.5.1.1 Para algoritmos de firma:
- 9.2.5.1.1.1 Algoritmos definidos en el “draft Representation of Public Keys and Digital Signatures in Internet X.509 Public Key Infrastructure Certificates” desarrollado por el PKIX Working group del Internet Engineering Task Force (IETF), excluyendo el MD”.
- 9.2.5.1.1.2 El algoritmo y la longitud de la clave seleccionados deben garantizar la unicidad de la firma digital de los documentos que se firmen de acuerdo con los usos permitidos del certificado. Esta longitud debe ser igual a 1024 bits en el algoritmo de RSA o su equivalente. Longitudes inferiores serán admitidas, pero no menores de 512 bits o su equivalente, previa justificación de garantía de la unicidad.
- 9.2.5.1.2 Para generación de par de claves un método de generación de claves privada y pública que garantice la unicidad y la imposibilidad de estar incurso en situaciones contempladas en el artículo 16 del decreto 1747 de 2.000.
- 9.2.5.1.3 Para generación de firma digital un sistema de generación de firma digital que utilice un algoritmo de firma digital admitido.

- 9.2.5.1.4 Para certificados en relación con firma digital, los certificados compatibles con el estándar de la International Telecommunication Union (ITU – T) X – 509 versión 3.
- 9.2.5.1.5 Para listas de certificados revocados el estándar de CRL de la ITU X – 509 versión 2.
- 9.2.5.2 La declaración de prácticas de certificación , debe estar accesible desde el “homepage” de la entidad de certificación, disponible al público en todo momento y debe incluir:
- 9.2.5.2.1 La identificación de la entidad que presta los servicios de certificación. La norma incluye los preceptos que la Superintendencia de Industria y Comercio considera deben ser incluidos en la “identificación”.
- 9.2.5.2.2 La política de manejo de los certificados, que debe incluir:
- 9.2.5.2.2.1 Los requisitos y el procedimiento de expedición de los certificados, incluyendo los procedimientos de identificación del suscriptor y de las entidades reconocidas, según el artículo 43 de la ley 527 de 1.999.
- 9.2.5.2.2.2 Los tipos de certificados que ofrece, sus diferencias, el grado de confiabilidad y los posibles usos de cada uno de ellos, límites de responsabilidad y el tiempo durante el cual se garantiza la condición de unicidad de la firma digital.

- 9.2.5.2.2.3 El contenido de cada uno de los distintos tipos de certificados.
- 9.2.5.2.2.4 El procedimiento para la actualización de la información contenida en los certificados.
- 9.2.5.2.2.5 El procedimiento, las verificaciones, la oportunidad y las personas que podrán invocar las causales de suspensión o revocación de los certificados.
- 9.2.5.2.2.6 La vigencia de cada uno de los tipos de certificados.
- 9.2.5.2.2.7 La información sobre el sistema de seguridad para proteger la información que se recoge con el fin de expedir los certificados.
- 9.2.5.2.3 Las obligaciones de la entidad de certificación y de los suscriptores del certificado y las precauciones que deben observar los terceros que confían en el certificado.
- 9.2.5.2.4 La información que se les va a solicitar a los suscriptores.
- 9.2.5.2.5 El manejo de la información que se obtiene de los suscriptores de acuerdo a las normas aplicables en la materia, detallando:
 - 9.2.5.2.5.1 El manejo de la información de naturaleza confidencial.
 - 9.2.5.2.5.2 Los eventos en que se revelará la información confidencial dada por el suscriptor, de acuerdo con las normas vigentes.
- 9.2.5.2.6 Las garantías que ofrece la entidad para el cumplimiento de las obligaciones que se deriven de sus actividades y los clausulados de los

seguros que protegen a los terceros por los perjuicios que pueda causar la entidad y/o los reglamentos de los contratos de fiducia constituidos para el efecto.

9.2.5.2.7 Los límites de responsabilidad de la entidad de certificación en cada uno de los tipos de certificados y por cada documento firmado.

9.2.5.2.8 Las tarifas de expedición y revocación de certificados y los servicios que incluyen.

9.2.5.2.9 Los procedimientos de seguridad para el manejo de:

9.2.5.2.9.1 Cuando la seguridad de la clave privada de la entidad de certificación se ha visto comprometida.

9.2.5.2.9.2 Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.

9.2.5.2.9.3 Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.

9.2.5.2.9.4 Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.

9.2.5.2.10 El plan de contingencia encaminado a garantizar la continuidad del servicio de certificación, en caso de que ocurra algún evento que comprometa la prestación del servicio.

9.2.5.2.11 Modelos y minutas de los contratos que utilizará.

9.2.5.2.12 La política de manejo de otros servicios que fuere a prestar, detallando sus condiciones.

9.2.5.3 Un sistema será confiable cuando cumpla con lo señalado en la presente resolución respecto de Políticas planes y procedimientos de seguridad, corta fuegos (Firewall) y sistemas de emisión y administración de certificados.

9.2.5.4 La entidad debe definir y poner en práctica las políticas, planes y procedimientos de seguridad tendientes a garantizar la prestación continua de los servicios de certificación, que deben ser revisados y actualizados periódicamente. Estos deben incluir al menos:

9.2.5.4.1 Políticas y procedimientos de seguridad en las instalaciones físicas y los equipos.

9.2.5.4.2 Políticas de acceso a los sistemas e instalaciones de la entidad, monitoreo constante.

9.2.5.4.3 Procedimientos de actualización de hardware y software, utilizados para la operación de entidades de certificación.

9.2.5.4.4 Procedimientos de contingencia de cada uno de los riesgos potenciales que atenten en contra del funcionamiento de la entidad según estudio que se actualizará periódicamente.

- 9.2.5.4.5 Plan de manejo, control y prevención de virus informático.
- 9.2.5.4.6 Procedimiento de generación de claves de la entidad de certificación que garantice que:
 - 9.2.5.4.6.1 Sólo se hace ante la presencia de los administradores de la entidad.
 - 9.2.5.4.6.2 Los algoritmos utilizados y la longitud de las claves utilizadas son tales que garanticen la unicidad de las firmas generadas en los certificados, por el tiempo de vigencia máximo que duren los mensajes de datos firmados por sus suscriptores.
- 9.2.5.5 La entidad de certificación debe aislar los servidores de la red interna y externa mediante la instalación de un corta fuegos o firewall, en el cual deben ser configuradas las políticas de acceso y alertas pertinentes. La red del centro de cómputo debe estar ubicada en segmentos de red físicos independientes de la red interna del sistema, garantizando que el corta fuegos sea el único elemento que permita el acceso lógico a los sistemas de certificación.
- 9.2.5.6 Los sistemas de emisión y administración de certificados deben prestar en forma segura y continua el servicio. Las entidades deben cumplir al menos con una de las siguientes condiciones:

- 9.2.5.6.1 Cumplir el certificate Issuing and Management Component Protection Profile nivel 2 desarrollado por el National Institute of Standards and Technologies; o
- 9.2.5.6.2 Cumplir con requerimientos técnicos que correspondan por lo menos con los objetivos del nivel de protección 2 (Evaluation Assurance Level 2) definido por Common Criteria for Information Technology Security Evaluation (CC 2.1) CCIMB-99-031 desarrollado por el Common Criteria Project Sponsoring Organization en su parte 3 o su equivalente en la norma ISO/IEC 15408, de:
- 9.2.5.6.2.1 Sistema de registro de auditoría de todas las operaciones relativas al funcionamiento y administración de certificados, que permita reconstruir en todo momento cualquier actividad de la entidad.
- 9.2.5.6.2.2 Sistema de almacenamiento secundario de toda la información de la entidad, en un segundo dispositivo que cuente por lo menos con la misma seguridad que el dispositivo original, para poder reconstruir la información de forma segura en caso necesario.
- 9.2.5.6.2.3 Dispositivo de generación y almacenamiento de la clave privada, tal que se garantice su privacidad y destrucción en caso de cualquier intento de violación, y

9.2.5.6.2.4 Sistema de chequeo de integridad de la información sistema, los datos y en particular de sus claves.

9.3 Certificados.

9.3.1 Los certificados deben cumplir con lo señalado respecto de los estándares y con los requisitos señalados en la Ley 527 de 1.999 respecto de su contenido.

9.3.2 Los certificados recíprocos deben contener al menos la siguiente información:

9.3.2.1 Identificador único del certificado.

9.3.2.2 Clave pública de la entidad que se está reconociendo.

9.3.2.3 Tipos de certificados a los que se remite el reconocimiento.

9.3.2.4 Duración del reconocimiento.

9.3.2.5 Referencia de los límites de responsabilidad del tipo de certificado al cual se remite el reconocimiento.

10. Sentencia 662 de 2.000.

10.1 En Junio 8 de 2.000, la Honorable Corte Constitucional profiere la sentencia 662 de 2.000. La sentencia referida, se suscita por el ejercicio de la acción pública de constitucionalidad, acción instaurada por Olga Lucía Toro Pérez

en contra de la Ley 527 de 1.999 y especialmente sus artículos 10, 11,12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45.

La actora, Olga Lucía Toro Pérez, solicita a la Corte Constitucional declarar inexecutable los artículos citados. El Magistrado sustanciador, Doctor Fabio Morón Díaz, mediante auto de Noviembre 19 de 1.999, admite la demanda y dispone traslado de la misma al señor Procurador General de la Nación para obtener el concepto de su competencia y comunica la iniciación del proceso al Presidente de la República, a los señores ministros de Comercio Exterior, Desarrollo Económico, Comunicaciones y Transporte, así como al Superintendente de Industria y Comercio.

Cumplidos los trámites constitucionales y legales propios de los procesos de inconstitucionalidad, la Corte Constitucional procede a decidir acerca de la demanda.

10.2 La Demanda: La demandante cuestiona el texto íntegro de la Ley 527 de 1.999 y, en especial, sus artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 por estimar que violan el artículo 131 de la Carta Política, así como los artículos 152 y 153.

La transgresión del artículo 131 se produce por cuanto la ley 527 de 1.999 crea unas entidades de certificación facultadas para emitir certificados en relación con las firmas digitales de las personas y para ofrecer los servicios de registro y estampado cronológico, la de certificación de la transmisión y recepción de mensajes de datos, así como cualquier otra de autenticación de firmas relativas a las comunicaciones basadas en firmas digitales, a emitir certificados en relación con la veracidad de firmas digitales de personas naturales o jurídicas y, en fin, realizar actos que según el entendimiento que da a la norma constitucional antes citada, es del resorte exclusivo de los Notarios, únicos depositarios de la fe pública.

En su criterio, *“lo que no permite la Constitución Política es que la autenticidad del documento privado sea función que pueda ejercer cualquier persona, por cuanto esta es una función propia del servicio público notarial y solo le puede corresponder al Notario, el cual siempre tiene que ser una persona natural, que llegue a serlo en propiedad o por concurso...”*. *“...si la ley asigna la función fedante a personas diferentes de los Notarios, infringiría en forma directa lo establecido en el artículo 131 de la Carta y esto es, precisamente lo que ha hecho la ley acusada, en especial en los artículos antes citados”*.

La actora argumenta igualmente, que se incurrió en violación de los artículos 152 y 153 de la Carta Política , pues los artículos 9, 10, 11, 12, 13, 14, 15 y 28 de la Ley 527 de 1.999 modificaron y adicionaron el Código de Procedimiento Civil, que según ella es equivalente a la administración de justicia, al conferir a los mensajes de datos la fuerza probatoria de que tratan las disposiciones del Capítulo VIII del Título XIII, Sección Tercera del Libro Segundo del Código de Procedimiento Civil(i); “ *ordenar que en toda actuación jurídica se dé eficacia, validez y fuerza obligatoria y probatoria a todo tipo de información emitida en forma de mensaje de datos(ii); y, finalmente, al disponer que los jueces deben aplicar a los mensajes de datos las reglas de la sana crítica al apreciarlos como prueba (iii).*”

10.3 Intervenciones Ciudadanas y de Autoridades Públicas: La Corte Constitucional encuentra que los argumentos de los intervinientes en defensa de la Ley 527 de 1.999, son coincidentes, por lo que los resume y unifica. Los argumentos son los siguientes:

10.3.1 El examen de constitucionalidad de la Ley debe tener en cuenta la trascendencia que el comercio electrónico tiene en la globalización de las relaciones económicas, el impacto de su evolución, las consecuencias que

genera en el desarrollo de los actos y negocios jurídicos celebrados, así como la importancia de regular y reglamentar jurídicamente su utilización.

10.3.2 La Ley 527 de 1.999 sigue los lineamientos del proyecto tipo de Ley modelo sobre comercio electrónico de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional – CNUDMI.

10.3.3 En el caso colombiano fue el producto de un proceso en el que participaron los sectores público y privado que tomaron parte en la comisión redactora.

10.3.4 El Comercio Electrónico encierra dentro de su filosofía los postulados de la buena fe comercial y de la libertad contractual entre los negociantes, principios que rigen todas y cada una de las transacciones realizadas mediante su utilización. Su regulación busca permitir el acceso de todas las personas a esta forma tecnológica de realizar transacciones de índole comercial y contractual.

10.3.5 Ni el comercio electrónico ni la actividad de las entidades de certificación son un servicio público, pues las partes no se encuentran en la obligación ni en la necesidad de solicitar los servicios de una entidad de certificación para la celebración de un negocio jurídico. Se trata de un asunto del Derecho Privado que, precisa de un control estatal que estará a cargo de la Superintendencia de Industria y Comercio, que vigila a las entidades de certificación desde el punto de vista técnico y operativo.

- 10.3.6 La Ley cuestionada apunta a proveer tanto a los mensajes de datos como al comercio electrónico de la integridad, confiabilidad y la seguridad que en este tipo de intercambio son cruciales, pues las partes actúan electrónicamente, a través de redes telemáticas, sin haber contacto físico.
- 10.3.7 Las firmas digitales, el certificado electrónico y el servicio de certificación prestados por las entidades de certificación son herramientas de índole eminentemente técnica que apuntan a dotar de seguridad a los mensajes de datos y el comercio electrónico.
- 10.3.8 Los cargos de la demanda resultan infundados porque las entidades de certificación no prestan un servicio público y menos dan fe pública. Las entidades de certificación no son notarías electrónicas, pues no sustituyen ni prestan los mismos servicios, según se deduce de la sola lectura del artículo 30 de la Ley 527 de 1.999 que relaciona las actividades que las primeras pueden realizar.
- 10.3.9 La actividad de certificación es un servicio de índole eminentemente técnico que tiene que ver con la confianza y la credibilidad y que propende por la seguridad en los mensajes de datos empleados lo que básicamente comprende: la inobjetablez de origen; la integridad de secuencia, la inobjetablez de recepción, la confidencialidad, la unicidad de fin y la temporalidad. Ello se logra a través de una entidad reconocida por un grupo

de usuarios, quien certifica sobre el iniciador de la información, que su contenido no ha sufrido alteraciones ni modificaciones y que fue recibida por su destinatario.

10.3.10 Ni la Constitución ni las leyes han establecido que las funciones públicas o los servicios públicos sólo pueden ser prestados por entidades o servidores públicos.

10.3.11 De ahí que, si las funciones de las entidades certificadoras fueren eventualmente calificadas como relacionadas con la fe pública, ello en momento alguno significa que el legislador dentro de su competencia no pueda atribuírselas a dichas entidades en su condición de entes privados, tal como lo ha hecho la ley con los notarios respecto de las funciones a ellos asignadas.

10.3.12 Si la actividad de las entidades de certificación se catalogase como servicio público, se trataría de uno diferente del que prestan las Notarías, y en todo caso su constitucionalidad estaría amparada por el por el artículo 365 de la Constitución. Debido a los desarrollos tecnológicos se consideró necesario proteger el derecho fundamental de los particulares a obtener información veraz (Art. 20 C.N), otorgar facultades relacionadas con la guarda de la fe pública a entidades certificadoras, desde una perspectiva

diferente a la de los notarios, no quiere decir que el legislador esté contraviniendo el artículo 131 de la Carta Política.

10.3.13 Puede ser cierto que la Ley 527 modificó algunas disposiciones contenidas en códigos, dichas modificaciones en ningún momento pueden llegar a considerarse que afectan la estructura general de la administración de justicia o los principios sustanciales y procesales sobre la materia.

10.3.14 La Ley 527 de 1.999 no modifica ni deroga una ley estatutaria y su tema no forma parte de la reserva atribuida a estas leyes, razón por la cual su trámite y aprobación no debía sujetarse a la mayoría absoluta de los miembros del Congreso, siendo procedente que su contenido fuera regulado a través de una ley ordinaria. Por ello es infundado el cargo de violación de los artículos 152 y 153 aunque la Ley 527 haya modificado el Código de Procedimiento Civil, de ello no se sigue que su contenido sea el propio de la Ley Estatutaria sobre la Administración de Justicia. En abundante jurisprudencia la Corte ha sostenido que no toda reforma procedimental puede entenderse como un cambio a la estructura misma de la Administración de Justicia. Sólo un cambio en su estructura o en sus principios sustanciales y procesales, deben ser regulados a través de legislación estatutaria. Por el contrario, las modificaciones procesales que no toquen esos principios, son del resorte de la ley ordinaria.

10.4 Concepto del Procurador General de la Nación: El Procurador General de la Nación rindió en tiempo su concepto y solicita declarar constitucional la Ley acusada. Respecto a la supuesta vulneración del artículo 131 considera que se debe a una particular interpretación, según la cual, el artículo 131 habría encargado de manera exclusiva a los notarios el servicio público de otorgar la fe pública.

Señala que no comparte esa interpretación pues en su concepto, el artículo 131 no consagra ni explícita ni implícitamente la pretendida exclusividad, ya que únicamente señala que le compete a la ley la reglamentación del servicio público que prestan los notarios y registradores. El resto del artículo 131 se refiere a la constitucionalización de la carrera notarial y la facultad gubernamental de crear los círculos de notariado y registro, sin que en parte alguna se prevea que la función de otorgar la fe pública sea de competencia exclusiva de los notarios. Lo que sí es claro, es que no puede deducirse que el Constituyente haya establecido que la actividad fedante sea privativa de los notarios. Es más, en el artículo 131 no existe referencia alguna, qué personas son las competentes para otorgar la fe pública.

Respecto a la supuesta violación de los artículos 151 y 152 considera infundado el argumento de inconstitucionalidad, según el cual la Ley 527 de

1.999 debió someterse a los trámites propios de una ley estatutaria. Recuerda que la Corte Constitucional ha sentado el criterio de acuerdo con el cual la exigencia constitucional de la reserva de la ley estatutaria, en el caso de las normas legales que se refieran a la administración de justicia, procede cuando la norma legal trate de asuntos concernientes a derechos fundamentales de las personas o a la estructura misma de dicha administración. No es exigible esa modalidad de legislación por la sola circunstancia que una determinada ley haga referencia a algunos de los temas respecto de los cuales el Constituyente previó el trámite especial contenido en el artículo 152 de la Carta.

10.5 Consideraciones y Fundamentos:

10.5.1 Competencia: En virtud de lo dispuesto en el artículo 241-4 de la Constitución, la Corte Constitucional es competente para decidir definitivamente sobre la demanda de inconstitucionalidad que dio origen al proceso.

10.5.2 El Contexto de la Ley 527 de 1.999

10.5.2.1 La revolución de los medios de comunicación de las dos últimas décadas a causa de los progresos tecnológicos en el campo de los computadores, la telecomunicaciones y la informática.

El Vicepresidente Ejecutivo (e) de la Cámara de Comercio de Bogotá, se refirió a los avances tecnológicos que ambientaron la regulación sobre mensajes de datos y comercio electrónico así como a su incalculable valor agregado en la expansión del comercio.

“La posibilidad de transmitir digitalmente la información de manera descentralizada, el desarrollo de Internet a finales de los años sesenta y el perfeccionamiento de sus servicios desde la aparición de la Red de Redes en los años ochenta, se constituyeron en los pilares básicos para el despegue del comercio electrónico.

En la actualidad el desarrollo del comercio electrónico a nivel mundial es un hecho innegable e irreversible. No sólo es así, sino que según se prevé, seguirá en crecimiento en los próximos años generando grandes ingresos a través de la red, el cual innegablemente causa un impacto sobre las actividades económicas, sociales y jurídicas en donde estas tienen lugar.

A pesar de no haber madurado aún, el comercio electrónico crece a gran velocidad e incorpora nuevos logros dentro del ciclo de producción.

A nivel general, todo parece indicar que este nuevo medio de intercambio de información, al eliminar barreras y permitir un contacto en tiempo y real entre consumidores y vendedores, producirá mayor

eficiencia en el ciclo de producción aparejado a un sin número de beneficios como la reducción de costos, eliminación de intermediarios en la cadena de comercialización, etc. Trayendo importantes e invaluable beneficios a los empresarios que estén dotados de estas herramientas.

En Colombia, las ventas por Internet son una realidad. Los centros comerciales virtuales y las transferencias electrónicas, entre otros, ya pueden encontrarse en la red. En 1.995 existían en nuestro país 50.000 usuarios de Internet, hoy, según estudios especializados, pueden llegar a los 600.000 y en el año 2.000 sobrepasarán el millón de suscriptores. Así las cosas, Colombia se perfila como uno de los países de mayor crecimiento en América Latina en utilización de recursos informáticos y tecnológicos para tener acceso a Internet y podría utilizar estos recursos para competir activa y efectivamente en el comercio internacional.”

10.5.2.2 La necesidad de actualizar los regímenes jurídicos, para otorgar fundamento jurídico al intercambio electrónico de datos.

Es indudable que los avances tecnológicos en materia de intercambio electrónico de datos ha propiciado el desarrollo de esta tendencia en todos los órdenes, lo cual implica hacer las adecuaciones en los

regímenes que sean necesarias para que estén acorde con las transformaciones que han tenido lugar en la organización social, económica y empresarial. *“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.”*

10.5.2.3 La Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil Internacional – CNUDMI.

La Comisión de las Naciones Unidas para el Desarrollo del derecho Mercantil promovió la gestación de un proyecto de ley tipo en materia de comercio electrónico, inspirada en la convicción de que al dotársele de fundamentación y respaldo jurídicos, se estimularía el uso de los mensajes de datos y del correo electrónico para el comercio, al hacerlos confiables y seguros.

El régimen legal formulado por la Comisión de Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional, busca ofrecer:

“ ...

al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitieran eliminar algunos de esos obstáculos jurídicos con miras a crear un marco jurídico que permitiera un desarrollo más seguro de las vías electrónicas de negociación designadas por el nombre de comercio electrónico.”

“ ...

La ley modelo tiene la finalidad de servir de referencia a los países en la evaluación y modernización de ciertos aspectos de sus leyes y prácticas en las comunicaciones con medios computarizados y otras técnicas modernas y en la promulgación de la legislación pertinente cuando no exista legislación de este tipo.”

Según consta el proyecto colombiano se basó en la Ley modelo de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional sobre Comercio Electrónico.

- 10.5.2.4 Los antecedentes de la Ley 527 de 1.999. Obedeció a la necesidad de que existiese en nuestra legislación un régimen jurídico acorde con las nuevas realidades en que se desarrollan las comunicaciones y el

comercio, para que las herramientas jurídicas y técnicas den un fundamento sólido y seguro a las relaciones y transacciones que se lleven a cabo por vía electrónica y telemática. Colombia se pone a tono con las modernas tendencias del derecho internacional privado.

Así la Ley 527 facilita el uso del intercambio electrónico de informaciones (EDI), y de medios conexos de comunicación de datos y concede igual trato a los usuarios de documentación con soporte de papel y a los usuarios de información con soporte informático.

10.5.3 Estructura de la Ley 527 de 1.999. Conociendo ya la estructura de la Ley 527 de 1.999 pues es el objeto del presente estudio, nos parece importantísimo seguir a la Corte Constitucional en la ilustración de los mensajes electrónicos de datos, las firmas digitales, las entidades de certificación y el alcance probatorio de los mensajes de datos.

10.5.3.1 Mensajes Electrónicos de datos. Se considera como la piedra angular de las transacciones comerciales telemáticas. Cuando en la definición de mensaje de datos se mencionan los “medios similares”, se busca establecer que la norma no está exclusivamente destinada a conducir las prácticas modernas de comunicación, sino que pretenden ser útiles para todos los adelantos tecnológicos que se generen en un futuro.

El mensaje electrónico debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, su misma eficacia jurídica.

Dentro de las características esenciales del mensaje de datos encontramos que es una prueba de la existencia y naturaleza de la voluntad de las partes de comprometerse; es un documento legible que puede ser presentado ante las entidades públicas y los tribunales; admite su almacenamiento e inalterabilidad en el tiempo; facilita la revisión y posterior auditoría con fines contables, impositivos y reglamentarios; afirma derechos y obligaciones jurídicas entre los intervinientes y es accesible para su ulterior consulta. En la Ley se hace hincapié en que los mensajes no sean alterados y así se satisfacen los sistemas de protección de la información como la Criptografía y las firmas digitales, al igual que las actividades de las entidades de certificación.

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.

10.5.3.2 Firmas Digitales. A través de la firma digital se pretende garantizar que un mensaje de datos determinado procede de una persona determinada, que ese mensaje no se ha modificado desde su creación y transmisión y que el receptor no pudiera modificar el mensaje recibido.

La Criptografía que es una rama de las matemáticas que se ocupa de transformar, mediante un procedimiento sencillo, mensajes en formas aparentemente inteligibles y devolverlas a su forma original. Mediante el uso de un equipo físico especial, los operadores crean un par de códigos matemáticos, una clave secreta o privada y una clave pública. La firma digital es el resultado de la combinación de un código matemático creado por el iniciador para garantizar la singularidad de un mensaje, que separa el mensaje de la firma digital y la integridad del mismo con la identidad de su autor. La firma digital debe cumplir las mismas funciones que la firma consignada en un papel. Sus funciones son:

- Identificar a una persona como el autor.
- Dar certeza de la participación exclusiva de esa persona en el acto de firmar.
- Asociar a esa persona con el contenido del documento.

Es evidente que la transposición mecánica de una firma autógrafa realizada sobre papel y replicada por el ordenador a un documento informático no es suficiente para garantizar los resultados de la firma autógrafa, por lo que se crea la necesidad de que existan establecimientos que certifiquen la validez de esas firmas. Estos establecimientos son los llamados entidades de certificación.

10.5.3.3 Entidades de certificación. Un ente público o privado con poderes de certificar, proporciona la seguridad jurídica a las relaciones comerciales por vía informática. La entidad de certificación expide certificados, los cuales son manifestaciones hechas como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las claves criptográficas y la integridad de un mensaje de datos.

La naturaleza de la función de las entidades de certificación se considera como la prestación de un servicio público. Los servicios públicos pueden ser prestados tanto por las entidades públicas como las privadas o conjuntamente. Si es un particular debe reunir los requisitos exigidos en la ley y debe contar con la aprobación de la Superintendencia, organismo rector para todos los efectos. Así, la Ley 527 prevé que las entidades de certificación pueden ser las Cámaras de Comercio y en general las personas jurídicas, públicas o privadas,

autorizadas por la Superintendencia de Industria y Comercio. Es importante señalar que para la Corte Constitucional las funciones de las entidades de certificación son consideradas como la prestación de un servicio público.

10.5.3.4 Alcance probatorio de los mensajes de datos. La ley 527 de 1.999 le otorga al mensaje de datos la calidad de prueba, permitiendo coordinar el sistema telemático con el sistema manual o documentario, encontrándose en igualdad de condiciones en un litigio o discusión jurídica, teniendo en cuenta para su valoración criterios como confiabilidad, integridad de la información e identificación del autor. Al valorar la fuerza probatoria de un mensaje de datos se debe tener presente la confiabilidad de la forma en que se haya generado, archivado o comunicado el mensaje, la confiabilidad de la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

10.5.4 Los cargos globales.

Los reparos sobre la constitucionalidad de la ley 527 de 1.999 son dos: que las entidades certificadoras, estarían dando fe pública en Colombia, cuando esta función está reservada constitucionalmente de manera exclusiva a los notarios, a la luz del artículo 131 de la Constitución (i), y que se

desconocieron los artículos 152 y 153 de la Carta Política al haberse modificado el Código de Procedimiento Civil por la vía de una ley ordinaria cuando, según su afirmación, ha debido hacerse por Ley Estatutaria.

10.5.4.1 La supuesta invasión de la función notarial y la libertad del Legislador para regular el servicio notarial.

La Corte afirma que para el esclarecimiento de los cargos lo relevante no es definir la naturaleza de la actividad que realizan las entidades de certificación, sino su valor probatorio, que es lo realmente relevante para el derecho, pues, ciertamente es el marco jurídico el que crea el elemento de confianza. La confianza es la variable crítica para incentivar el desarrollo progresivo de las vías electrónicas de comunicación conocidas como correo electrónico y comercio electrónico, pues es el elemento que permite acreditarlos como un medio seguro, confiable y apto para facilitar las relaciones entre las personas.

El servicio de certificación propende proporcionar seguridad jurídica a las transacciones comerciales por vía informática, actuando la entidad de certificación como tercero de absoluta confianza, para lo cual la ley le otorga importantes prerrogativas de certificación técnica, entendiéndose por tal la que versa sobre las características técnicas en las que fue emitido

el mensaje de datos y sobre la comprobación de la identidad del emisor y del receptor.

A diferencia de los documentos en papel, los mensajes de datos deben ser certificados técnicamente para que cumplan funciones equivalentes a las de un documento tradicional o en papel. Las entidades de certificación certifican técnicamente que un mensaje de datos cumple con los elementos esenciales para considerarlo como tal, a saber, la confidencialidad, la autenticidad, la integridad y la no repudiación de la información, lo que en últimas permite inequívocamente tenerlo como auténtico.

La confidencialidad son los requisitos técnicos mínimos necesarios para garantizar la privacidad de la información.

La autenticidad es la certificación técnica que identifica a la persona iniciadora o receptora de un mensaje de datos.

La integridad es el cumplimiento de los procedimientos técnicos necesarios que garanticen que la información enviada por el iniciador es la misma del que lo recibió.

La no repudiación es el procedimiento técnico que garantiza que el iniciador de un mensaje no puede desconocer el envío de determinada información.

La Corte deshecha los cargos pues considera que la demandante confunde la competencia que el legislador tiene para reglamentar el servicio público que prestan los notarios y registradores, con la asignación a estos de la función fedante como una atribución constitucional privativa y excluyente. Así mismo, la Corte considera que el legislador está constitucionalmente habilitado para conferir el ejercicio de funciones públicas a los particulares con lo que la facultad que la Ley 527 de 1.999 otorga a las personas jurídicas privadas a prestar el servicio de certificación no vulnera el artículo 131 de la Constitución Nacional. Entrar a calificar como función pública o servicio público las atribuciones que la Ley 527 de 1.999 otorgó a las certificadoras no es asunto relevante.

10.5.4.2 Los acusados artículos 9º a 15 y 28 y la supuesta violación de los artículos 151 y 152 de la Constitución Política.

La demandante afirma que los artículos citados modifican y adicionan el Código de Procedimiento Civil en cuanto a los medios de prueba y a su valor probatorio, lo que en su sentir ha debido hacerse mediante el trámite y las mayorías propias de una Ley Estatutaria, por cuanto implica una reforma a la Ley Estatutaria de la Administración de Justicia.

La Corte considera que ese cargo se basa en una premisa equivocada. La reserva de Ley Estatutaria no significa que toda regulación que se relacione con los temas previstos en el artículo 152 de la Carta Constitucional deba someterse a dicho trámite especial. La Corte considera que debe considerarse para este caso lo previsto en la Sentencia C-037 de Febrero 5 de 1.996 en la que dijo:

“...Para la Corte, una ley estatutaria encargada de regular la administración de justicia, como lo dispone el literal b) del artículo 152 superior, debe ocuparse esencialmente sobre la estructura general de la administración de justicia y sobre los principios sustanciales y procesales que deben guiar a los jueces en su función de dirimir los diferentes conflictos o asuntos que se someten a su conocimiento.

De conformidad con lo anterior, esta Corporación entiende que el legislador goza, en principio de la autonomía suficiente para definir cuáles aspectos del derecho deben hacer parte de este tipo de leyes. Sin embargo, debe señalarse que esa habilitación no incluye la facultad de consagrar asuntos o materias propias de los códigos de procedimiento, responsabilidad esta que se debe asumir con base en lo dispuesto en el numeral 2º del artículo 150 superior, es decir, a través de las leyes ordinarias. Con todo, debe reconocerse que no es asunto

sencillo establecer una diferenciación clara y contundente respecto de las materias que deben ocuparse uno y otro tipo de leyes. Así pues, resulta claro que, al igual que ocurre para el caso de las leyes estatutarias que regulan los derechos fundamentales (literal A del artículo 152), no todo aspecto que de una forma o de otra se relacione con la administración de justicia debe necesariamente hacer parte de una ley estatutaria. De ser ello así, entonces resultaría nugatoria la atribución del numeral 2º del artículo 150 y, en consecuencia, cualquier código que en la actualidad regule el ordenamiento jurídico, o cualquier modificación que en la materia se realice, deberá someterse al trámite previsto en el artículo 153 de la Carta.

Reitera la Corte Constitucional que el propósito de las Leyes Estatutarias no es el de regular en forma exhaustiva la materia que constituye su objeto.

De esta manera, la Corte Constitucional, declara exequibles los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1.999.

CONCLUSIONES

Al finalizar nuestro trabajo de tesis podemos concluir entre otras cosas las siguientes:

1. La Ley 527 de 1.999, el Decreto 1747 de 2.000 y la Resolución 26930 de 2.000 son ejemplo de la innovación legislativa colombiana. Son prueba fehaciente de la manera en que el derecho evoluciona acomodándose a nuevas circunstancias y necesidades.
2. Colombia, a través de los mencionados cuerpos legislativos se pone a la vanguardia en materia de legislación electrónica.
3. El desarrollo de las entidades de certificación en nuestro país no ha sido importante pero suponemos que la necesidad de las mismas hará que en muy corto tiempo encontremos entidades certificadoras a lo largo y ancho del territorio nacional.
4. La Ley 527 de 1.999 es el instrumento que genera confianza entre los particulares que día a día utilizan con más frecuencia los medios electrónicos como instrumento para enviar y recibir ofertas y realizar negocios.

5. Al tenor de lo dispuesto en el artículo 252 de nuestro Código de Procedimiento Civil, “Es auténtico un documento cuando existe certeza sobre la persona que lo ha elaborado, manuscrito o firmado”. Así las cosas, habrá oportunidades en las que una persona que realiza actividades comerciales mediante documentos electrónicos, deba acudir a la justicia para que, por ejemplo, el juez declare que se extinguió una obligación comercial convenida electrónicamente. Como en cualquier otro proceso, el demandante al poner en práctica el aparato jurisdiccional, tendrá que acreditar la prueba de la existencia del contrato o de la operación comercial realizada electrónicamente.

Como es bien sabido por todos nosotros, probatoriamente no basta afirmar la existencia de un hecho y alegar innumerables normas jurídicas para obtener una decisión favorable, sino que es prácticamente indispensable que el litigante convenza al juez a través de su actividad probatoria. Con la expedición de la Ley de Comercio Electrónico y con los cuerpos legislativos que la han reglamentado, gran parte del problema probatorio ha desaparecido. La ley le otorga a los documentos electrónicos el mismo valor probatorio que tiene cualquier otro documento siempre y cuando éste cumpla con todos los requisitos de forma establecidos en ella. Más aún, sobraría el testimonio del comerciante generador o receptor de un documento electrónico si por medio nos encontramos con la actividad de una entidad certificadora, la cual no hace

sino certificar que el documento que originó el consentimiento contractual fue enviado desde el equipo del comerciante A y fue debidamente recibido por el comerciante B.

Creemos que el mérito probatorio del documento electrónico, una vez demostrada su autenticidad, al cumplir con los requisitos señalados en la Ley de Comercio Electrónico y normas complementarias, debe ser el de plena prueba de los hechos y declaraciones en él contenidos, claro está, salvo prueba en contrario.

En este orden de ideas, nos parece imprescindible traer a colación el tema relativo a la firma digital, debidamente certificada a través de la actividad de un tercero de buena fe como sería una entidad certificadora, quien por medio de su especialidad certifica que una “clave” pertenece exclusivamente a un sujeto. Ese documento, constituye plena prueba en los términos establecidos en el artículo 252 del Código de Procedimiento Civil, por lo que le corresponde al demandado probar las circunstancias por las cuales no lo es. Por ejemplo, que el mensaje fue firmado utilizando una clave privada que habiendo sido extraviada fue utilizada por un tercero antes de la cancelación que de ella debe hacer la entidad certificadora, etc.

La importancia de las normas analizadas a través del presente escrito, es que reglamentan la utilización del comercio electrónico como generador de actos

jurídicos, y crean las circunstancias particulares para que tales documentos produzcan los efectos jurídicos que las partes quieren generar con su utilización.

Todo lo anterior trae como consecuencia que la práctica del comercio electrónico no pierda su eficiencia y bajos costos, a la vez que genera certeza jurídica entre quienes lo utilicen.

Consideramos que lo más importante para lograr una apreciación de los documentos electrónicos como prueba de los hechos y los contratos ejecutados en el ciberespacio, es, principalmente, que los jueces amplíen sus criterios en base a los adelantos de la tecnología informática, pues de nada servirá que las partes utilicen los avances de la ciencia y de la tecnología como medio de prueba, si quienes están encargados de la resolución de sus conflictos, no tienen capacidad para apreciarlos en todo su valor probatorio, por desconocimiento o desconfianza.

Finalmente pensamos que la utilización universal del comercio electrónico debe llevar tarde o temprano a la globalización de la legislación que lo regula, con lo que indudablemente desaparecería el temor que aún existe en ciertas personas y grupos culturales de utilizarlo en mayor escala.

6. Es importante analizar igualmente, las consecuencias jurídicas que se derivan de la utilización generalizada del internet, en cuanto a establecimiento de comercio, contratos derivados del mundo web y una nueva especie de títulos valores, los títulos valores electrónicos.
- 6.1. Establecimiento de Comercio: De acuerdo con el artículo 515 del Código de Comercio, “Se entiende por establecimiento de Comercio un conjunto de bienes organizados por el empresario para realizar los fines de la empresa. Una misma persona podrá tener varios establecimientos de comercio y, a su vez, un solo establecimiento de comercio podrá pertenecer a varias personas, y destinarse al desarrollo de diversas actividades comerciales.” (12). El artículo 516 del mismo cuerpo legal establece que salvo estipulación legal en contrario, se entiende que forman parte de un establecimiento de comercio: “1. La enseña o nombre comercial y las marcas de productos y de servicios; 2. Los derechos del empresario sobre las invenciones o creaciones industriales o artísticas que se utilicen en las actividades del establecimiento; 3. Las mercancías en almacén o en proceso de elaboración, los créditos y los demás valores similares; 4. El mobiliario y las instalaciones; 5. Los contratos de arrendamiento y, en caso de enajenación, el derecho al arrendamiento de los locales en que funciona si son de propiedad del empresario, y la indemnizaciones que, conforme a

la ley, tenga el arrendatario; 6. El derecho a impedir la desviación de la clientela y la protección de la fama comercial, y 7. Los derechos y obligaciones mercantiles derivados de las actividades propias del establecimiento, siempre que no provengan de contratos celebrados exclusivamente en consideración al titular de dicho establecimiento.”(13).

Es posible aplicar las nociones de establecimiento de comercio a un sitio de internet y por analogía los elementos que lo conforman para que la legislación comercial cubra, regule y ampare los sitios web? En nuestra opinión sí es posible. Analizamos entonces los elementos que según nuestra legislación comercial hacen parte del establecimiento de comercio para concluir sin lugar a dudas que un sitio web, es un establecimiento de comercio:

- 6.1.1 Nombre Comercial o enseña: Según el artículo 583 del Código de Comercio, “se entiende por enseña, el signo que utiliza una empresa para identificar su establecimiento” y “se entiende por nombre comercial el que designa al empresario como tal”. (14). Fácilmente podemos colegir, que el nombre de dominio utilizado por el comerciante virtual, es una enseña, ya que los navegantes de la red deben ingresar a esa página o sitio específico para acceder a los productos, bienes o servicios, que nuestro comerciante virtual ofrece. Lo mismo podríamos afirmar del nombre comercial. Creemos

importante remitirnos en éste aspecto a lo establecido en la Decisión 486 de la Comunidad Andina, aplicable en Colombia, Ecuador, Perú, Bolivia y Venezuela a partir del 1º de Diciembre de 2.000, la que establece una acción de cancelación de nombre de dominio. La persona que puede accionar es quien es titular de un signo distintivo notoriamente reconocido contra un tercero que ha inscrito o registrado indebidamente el signo de aquel en alguno de los países miembros de la Comunidad. Quien hace la cancelación del dominio es la autoridad nacional competente y lo hace si produce alguno de los efectos siguientes: a) "riesgo de confusión o de asociación con el titular del signo, o con sus establecimientos, actividades, productos o servicios; b) daño económico o comercial injusto al titular del signo por razón de una dilución de la fuerza distintiva o del valor comercial o publicitario del signo; o c) aprovechamiento injusto del prestigio o renombre del signo". (15).

6.1.2 Marcas de Productos y Servicios e Invenciones o Creaciones Industriales o Artísticas: Cada día es más importante la identificación de las marcas en el mundo del Internet, porque esa seguridad para el comprador le da la certeza de adquirir específicamente el bien que está buscando y que no puede ser reemplazado por uno similar y posiblemente de menor calidad al que requiere. Es más, en un mundo tan competitivo como el ciberespacio,

los signos distintivos de cada empresa son esenciales. En cuanto a las creaciones industriales, consideramos que estamos frente a una clase específica de propiedad industrial y que un comerciante virtual puede adquirir derechos exclusivos de patente, siempre y cuando cumpla con los requisitos establecidos en la ley para las invenciones. En cuanto a las creaciones artísticas o del intelecto, estamos seguros que el comerciante virtual que utilice creaciones artísticas en su página web debe estar sometidos a la legislación que regula los derechos de autor y debe cumplir con las obligaciones que de ella se derivan, verbi gracia, pago de derechos de autor, etc.

- 6.1.3 Las mercancías en almacén o en proceso de elaboración y los créditos y demás valores similares: Debe ser fácilmente comprobable que el comerciante de internet posea un stock de mercancías en almacén con el objeto de atender las compras que a través de su página web le hagan los internautas, las que una vez confirmadas debe atender haciendo despachos a nivel nacional e internacional. En cuanto a los créditos creemos que la compra hecha en línea es una compra inmediata, pero pueden quedar saldos para aplicar a esa compra, si el despacho es internacional y condicionan el pago al momento en que el comprador reciba a entera satisfacción el producto en el país de destino, y aún cuando se

haga una compra mediante un medio electrónico de pago en el que se difiera el mismo en varias cuotas.

6.1.4 Contratos de Arrendamiento: Cuando una persona diseña y da a la luz pública un sitio de internet, lo hace a través de un contrato de hosting, el cual, por sus características equivale a un contrato de arrendamiento.

6.1.5 Derecho a reprimir la Competencia Desleal: De acuerdo con lo establecido en el artículo 7° de la Ley 256 de 1.996, para que exista un acto de competencia desleal se requiere: “a) Que el acto se realice en el mercado, b) Que se lleve a cabo con fines concurrenciales y c) Que sea contrario a las sanas costumbres mercantiles, al principio de buena fe comercial, a los usos honestos en materia industrial o comercial y cuando esté encaminado a afectar, o afecte la libertad de decisión del comprador o consumidor, o el funcionamiento concurrencial en el mercado”. (16). Así pues, el comerciante que es propietario de un establecimiento electrónico tiene todas las garantías previstas en la Ley 256 de 1.996 y, en consecuencia, puede acudir a la Superintendencia de Industria y Comercio, o a los jueces para hacer valer sus derechos en ésta materia. Nos queda la duda, en caso que la competencia desleal sea consecuencia de actos provenientes de actuaciones que se generen en el extranjero. Por ello la importancia clara y necesaria de lograr una legislación universal que regule la materia.

Como se puede apreciar, al comerciante de internet y a su negocio virtual se aplican todos los elementos que nuestro Código de Comercio establece en relación con un establecimiento de comercio, por lo que es fácil concluir, que estamos sin lugar a dudas frente a uno de ellos. Así pues, por analogía debemos concluir necesariamente que nuestro comerciante virtual debería cumplir con los requisitos, deberes y obligaciones establecidos en nuestra legislación mercantil para un establecimiento de comercio. Debe cumplir con la obligación de inscribirlo en el registro mercantil, así como sus libros y demás obligaciones en el artículo 19 del Código de Comercio. Sin embargo, surge una inquietud, en relación con las páginas web que tienen su asiento en otros países del mundo y que, por la universalidad del ciberespacio generan negocios mercantiles con usuarios colombianos. Será necesario para ellos establecer una sucursal en Colombia con el lleno de los requisitos establecidos en nuestra legislación mercantil? A nuestro modo de ver ello sería necesario pero en la práctica ello aún no ocurre. Otra prueba más de la necesidad de regular la materia universalmente y que nuestro legislador acoja dicha legislación de manera inmediata.

6.2. Contratos que se derivan del Internet:

Otro aspecto sustancial en relación con la materia que nos ocupa, es que debido a la globalización del ciberespacio, surgen distintos tipos

contractuales que aún no han sido regulados de manera expresa por nuestra legislación y que generan obligaciones y derechos de diversa índole. Estos contratos al no estar regulados expresamente en nuestra legislación podrían considerarse atípicos. Lo cierto es que no es difícil imaginar que a la fecha, algunos de ellos hayan generado conflictos judiciales por el incumplimiento que alguna de las partes haya hecho de ellos.

En ese orden de ideas, los jueces que diriman los procesos derivados de esos contratos deben acudir a las teorías de la analogía, combinación o absorción para interpretarlos. (17).

Estos contratos podemos resumirlos en los siguientes: Contrato de Acceso a Internet, contrato para la obtención de un nombre de dominio, contrato para el diseño y desarrollo de un sitio web, contrato de hosting u hospedaje, contrato de e-marketing, contrato de pago de obligaciones electrónicas, y muchos otros que por no ser el tema principal de la presente investigación no entraremos a analizar, pero que deben convertirse en centro de atención para nuestro legislador, pues en muy corto tiempo serán los contratos típicos por excelencia, dejando a un lado a muchos otros que por el desarrollo de las ciencias y la tecnología, se convertirán en obsoletos.

6.3. Título valor Electrónico: Por último, creemos conveniente analizar una nueva forma de título valor, cuya utilización es bastante reciente. El Título Valor Electrónico. De acuerdo con lo establecido en el artículo 619 del Código de Comercio, “los títulos-valores son documentos necesarios para legitimar el ejercicio del derecho literal y autónomo que en ellos se incorpora. Pueden ser de contenido crediticio, corporativos o de participación, y de tradición o representativos de mercancías.” (18). De acuerdo con la anterior descripción y al tenor de lo dispuesto en los artículos 648, 651 y 668 del Código de Comercio es imprescindible al hablar de la ley de circulación de los títulos valores nominativos, a la orden o al portador sea necesaria la entrega real y material del título. Lo anterior nos lleva necesariamente a sostener que el título valor es un bien corpóreo y tangible.

Sin embargo, a partir de la expedición del Decreto 436 de 1.990, la Ley 27 de 1.990, el Decreto 437 de 1.992, la Resolución 1200 de 1.995, por parte de la Superintendencia de Valores, mediante la cual se reglamenta lo relativo al Depósito Centralizado de Valores y la posterior expedición de la Ley 527 de 1.999 o Ley de Comercio Electrónico, surge en el ámbito jurídico una nueva clase de título valor, el Título Valor Electrónico. A ese respecto nos parece importante referirnos someramente a las

características propias de estos títulos valores ya que con la expedición de nuestra Ley 527 de 1.999, toman fuerza, adquieren protagonismo y seguridad en el mundo del comercio.

6.3.1. Documento: “ Las bases de datos, archivos, centros de procesos, registros automatizados, registros electrónicos y mensajes operados electrónicamente a través de claves técnicas, son el soporte esencial para la existencia del Título Valor Electrónico: sistemas electrónicos que permiten incorporar el derecho, constituyendo una unidad, un matrimonio indisoluble. Derecho incorporado sin mensaje de datos no existe (documento electrónico o informático); mensaje de datos sin derecho no existe.” (19).

6.3.2. Literalidad: El depósito Centralizado de Valores se encarga de reproducir electrónicamente el título valor, permitiendo a cualquier persona, consultar el tenor literal del título y adquirirlo sin necesidad de que haya un desplazamiento físico, ni de la persona ni del título reproducido. Al analizar este punto, nos parece importante mencionar la opinión de Ricardo León Carvajal y Martha Cecilia Giraldo, en su libro el Título Valor electrónico ya que hacen alusión adecuadamente, a lo establecido en el artículo 626 del Código de Comercio colombiano y lo adaptan a las necesidades del Título Valor Electrónico: “ El suscriptor de un título quedará obligado conforme al

tenor literal del mismo, a menos que firme con salvedades compatibles con su esencia”, es el texto original que ellos modifican así: “ El suscriptor (firma digital) de un título valor electrónico quedará obligado conforme al tenor literal del mensaje de datos (manifestación de voluntad), a menos que se firme digital o electrónicamente con salvedades compatibles con su esencia”.

6.3.3. Autonomía: Consiste en que el último tenedor del título valor electrónico se obliga independientemente, al tenor de lo dispuesto en el artículo 627 del Código de Comercio, que reza: “ Todo suscriptor de un título valor se obligará autónomamente. Las circunstancias que invaliden la obligación de alguno o algunos de los signatarios, no afectarán las obligaciones de los demás.”(21). En el punto de la autonomía, nos parece importante resaltar lo afirmado por el doctor Gilberto Peña Castrillón, en su ponencia durante el VI Encuentro Latinoamericano de Expertos en Seguridad Bancaria; “En este punto la novedad es el evidente fortalecimiento de la autonomía, esto es, de la independencia del derecho de cada nuevo adquirente de un título valor remodelado electrónicamente, porque ahora cada nueva negociación acarrea una verdadera creación del título valor, terreno en el que resultaron inesperadamente útiles los títulos al portador como sucedió en España, circunstancia que independiza totalmente el derecho que surge para cada

nuevo adquirente, respecto de lo que hubiera podido ocurrir en las negociaciones precedentes. Por lo anterior el efecto práctico de toda esta experiencia cambiaria de porte electrónico es la incuestionable salvaguardia y fortalecimiento del principio de la autonomía que constituye, precisamente, la finalidad de la lucha por los títulos valores”.(22).

6.3.4. Legitimación: De acuerdo con lo establecido en el artículo 3.9.2.2 de la resolución 1.200 de 1.995, los certificados expedidos por el Depósito Centralizado de Valores, de conformidad con sus asientos electrónicos, legitiman al tenedor para exigir el cumplimiento de la obligación que incorpora el título valor electrónico: “Como documento de legitimación, el certificado sólo acreditará la situación del tenedor legitimado para exigir el cumplimiento de la obligación y lo exonera de presentar otra prueba de la titularidad del derecho que pretende ejercitar.”

6.3.5. Incorporación: El principio de la incorporación establecido en los artículos 619, 628, 629 y 654 de nuestro Código de Comercio, el que básicamente hace alusión a que la declaración de voluntad de quien se obliga debe quedar contemplado en un documento físico, corpóreo o mueble, para el caso de los títulos valores tradicionales, cambia en tratándose de Títulos Valores Electrónicos, pues su corporeidad no es otra que un mensaje de

datos, teniendo en cuenta desde luego, los elementos técnicos necesarios para crear, transmitir y verificar el Título Valor Electrónico.

CITAS BIBLIOGRAFICAS

1. SCHULTZE, "Zur Lehre vom Unkundenbeweise", Zeitschrift für das privat und öffentliche Recht der Gegenwart, vol. XXIII, (1.895), págs. 70 y ss.
2. PRIETO CASTRO, Manual de Derecho Procesal Civil I, Zaragoza, 1954, pág 331.
3. GUASP JAIME, Derecho Procesal Civil, 2ª ed., Madrid, 1.961, pág 405.
4. LOPEZ PALOP, Legislación Notarial, pág 314.
5. Corte Suprema de Justicia, Sentencia de Octubre 8 de 1.997.
6. Corte Suprema de Justicia, Sentencia de Octubre 8 de 1.997.
7. Corte Suprema de Justicia, Sentencia de Octubre 8 de 1.997.
8. CARNELUTTI, Sistema de Derecho Procesal Civil, t II, trad. Esp., Buenos Aires, 1.944, pág 417.
9. CARNELUTTI, Sistema de Derecho Procesal Civil, t II, trad. Esp., Buenos Aires, 1.944, pág 417.
10. MUÑOZ SABATE, Técnica Probatoria, Editorial Temis, 1.997, pág. 405.
11. GUASP JAIME, Derecho Procesal Civil, 2ª Ed. Madrid, 1.961, pág 407.
12. Código de Comercio Colombiano, artículo 515.
13. Código de Comercio Colombiano, Artículo 516.
14. Código de Comercio Colombiano, Artículo 583.

15. Decisión 486 de la Comisión de la Comunidad Andina. Publicado en la página de Internet. www.comunidadandina.com.
16. LEY 256 DE 1.996.
17. RENGIFO Ernesto, Derecho de la Distribución Comercial, El Navegante Editores, Biblioteca Milenio, Bogotá, 1.995. pág. 96.
18. Código de Comercio Colombiano. Artículo 619.
19. CARVAJAL MARTINEZ Ricardo, GIRALDO GOMEZ Marta Cecilia, Título Valor Electrónico. Señal Editora, 1.999. pág. 29.
20. Ibidem, pág. 37.
21. Código de Comercio Colombiano, Artículo 627.
22. PEÑA CASTRILLON Gilberto, Hacia una Nueva Concepción del Título Valor. Ponencias del VI Encuentro Latinoamericano de Expertos en Seguridad Bancaria, Bogotá, 1.991, pág. 12.
23. Resolución 1.200 de 1.995. Artículo 3.9.2.2.

BIBLIOGRAFIA

- MUÑOZ SABATE, Técnica Probatoria, Editorial Temis, 1997.
- SCHULTZE, "Zur Lehre vom Unkundenbeweise", Zeitschrift für das privat und öffentliche: Recht der Gegenwart, vol. XXIII, 1.865.
- PRIETO CASTRO, Manual de Derecho Procesal Civil I, Zaragoza, 1954.
- GUASP JAIME, Derecho Procesal Civil, 2ª Edición, Madrid, 1.961.
- LOPEZ PALOP, Legislación Notarial.
- CARNELUTTI, Sistema de Derecho Procesal Civil, tomo II, trad. Esp., Buenos Aires, 1.944.
- Corte Suprema de Justicia, Sentencia de Octubre 8 de 1.997.
- Corte Constitucional, Sentencia C-662/2.000.
- Ley 527 de 1.999
- Decreto 1747 de 2.000.
- Resolución 26930 de 2.000.
- Código de Comercio Colombiano.
- Decisión 486 de la Comisión de la Comunidad Andina.
- Ley 256 de 1.996.

- RENGIFO Ernesto, Derecho de la Distribución Comercial, El Navegante Editores, Biblioteca Milenio, Bogotá, 1.995.
- CARVAJAL MARTINEZ Ricardo, GIRALDO GOMEZ Marta Cecilia, Título Valor Electrónico. Señal Editora, 1.999.
- PEÑA CASTRILLON Gilberto. Hacia una Nueva Concepción del Título Valor. Ponencias del VI Encuentro Latinoamericano de Expertos en Seguridad Bancaria. Bogotá, 1.991.
- Resolución 1.200 de 1.995. Superintendencia de Valores.

