

A medio de prueba en todas las eventualidades en que sea necesario. A manera de ejemplo vemos los siguientes eventos: incontinuidad entre lo ofertado y lo entregado; incremento en el pago por error en la facturación y cargo en cuenta del cliente; plazo para la entrega a través del despacho por medios tradicionales, etc.

LA LEY

EL DOCUMENTO ELECTRÓNICO COMO MEDIO DE PRUEBA

DR.: JUAN BAUTISTA PARADA CAICEDO

Introducción

La evolución del comercio electrónico en nuestro país, acorde con el proceso de globalización de nuestra economía, ha desatado la dinámica de nuestras autoridades y como consecuencia de ella el gobierno ha llevado al Congreso el correspondiente proyecto de ley que regula la actividad y ha dado origen a la Ley 527 de 1999 "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

De todos es sabido que el comercio electrónico va dirigido esencialmente al consumo razón que impone la necesidad de tener en cuenta los aspectos jurídicos del contrato en sus diferentes etapas, a saber: oferta, modificación de la oferta, aceptación de la oferta, perfeccionamiento del contrato y cumplimiento del mismo.

Estas etapas del contrato pueden cumplirse en tiempo real o de forma diferida. Ejemplo del cumplimiento de las primeras en tiempo real es la oferta de software la cual es aceptada de inmediato, pagada y con entrega del producto al instante a través de la red. De manera diferida podemos ejemplificar con la oferta de productos aceptada por el consumidor, pagada a través de la red, todo ello en tiempo real y con envío y entrega posteriores por los medios de transporte tradicionales.

Estas operaciones realizadas en su esencia por medios electrónicos requieren, para seguridad de los usuarios, de documentos que sirvan de

medio de prueba en todas las eventualidades en que sea necesario. A manera de ejemplo veamos los siguientes eventos: Inconformidad entre lo ofertado y lo entregado; incremento en el pago por error en la facturación y cargo en cuenta del tarjeta-habiente; plazo para la entrega a través del despacho por medios tradicionales, etc.

LA LEY

Nuestra ley, siguiendo los modelos de la globalización y las políticas y recomendaciones de entidades como la UNCITRAL (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional), la OMPI (Organización Mundial de la Propiedad Intelectual) OMC (Organización Mundial del Comercio) pretende regular de manera eficiente el comercio electrónico en nuestro país y en sus antecedentes se recomienda que su interpretación se haga con criterios de globalización, esto es, siguiendo los precedentes de otros países que han logrado un mayor desarrollo en la actividad y, en consecuencia, han afrontado ya problemas que aún no proceden entre nosotros.

En la exposición de motivos del proyecto presentado al Congreso de la República por los Ministros de Justicia y del Derecho, de Desarrollo, de Comercio Exterior y de Transporte, que culminó en la expedición de la Ley 527 de 1999, ilustró las exigencias que el cambio tecnológico planteaba en términos de la actualización de la legislación nacional para ponerla a tono con las nuevas realidades de comunicación e interacción imperantes y para darle fundamento jurídico a las transacciones comerciales efectuadas por medios electrónicos y fuerza probatoria a los mensajes de datos, en los siguientes términos¹:

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...".

¹ Gaceta del Congreso No. 44, viernes 24 de abril de 1998, pp. 26 y ss.

La Asamblea General de la ONU, mediante Resolución 51/162 de 1996 aprobó la Ley Modelo sobre Comercio Electrónico elaborada por la CNUDMI y recomendó su incorporación a los ordenamientos internos como un instrumento útil para agilizar las relaciones jurídicas entre particulares.

El régimen legal modelo formulado por la Comisión de Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional –CNUDMI– 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 tipo²...”.

CONSTITUCIONALIDAD DE LA LEY.

La ley fue sometida a examen por la Corte Constitucional al despachar sendas demandas en su contra. La primera se despachó con la Sentencia C-662-00 con ponencia del Magistrado Fabio Morón Díaz. Referencia: expediente D-2693.

Acción pública de inconstitucionalidad contra la Ley 527 de 1999 y, particularmente 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 medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

Actora: Olga Lucía Toro Pérez

² Exposición de motivos, Supra.

Temas:

- El reconocimiento jurídico de la validez plena y del valor probatorio de los mensajes de datos
- El Comercio Electrónico
- La firma digital
- Las entidades de certificación y la emisión de certificados sobre la autenticidad de los mensajes de datos y las firmas digitales
- La actividad de las entidades de certificación y la función notarial.

La otra demanda fue decidida mediante la Sentencia C-831/01 Referencia: expediente D-3371 Demanda de inconstitucionalidad contra el artículo 6º de la Ley 527 de 1999. Actor: Daniel Peña Valenzuela. Magistrado Ponente: Dr. ÁLVARO TAFUR GALVIS.

La Ley 527/99 o ley de comercio electrónico, sigue la moderna tendencia de las legislaciones continentales europeas de introducir en su articulado las definiciones del sentido de las palabras que se van a utilizar, "... técnica inglesa que según Radbruch, estaba dirigida a evitar la disolución de las leyes del Parlamento, el Statute Law, en el tejido unitario del Common Law, por la vía interpretativa de los Tribunales". En sus palabras: "Los Statutes son interpretados con el espíritu de la Common Law y quedan muy pronto transformados por una espesa capa de precedentes normativos, y de este modo entretejidos inseparablemente en el tejido unitario de la Common Law. Es verdad que el Parlamento, por su parte, toma demasiadas medidas contra el peligro de que, por virtud de tales artes interpretativas, la ley pierda su espíritu y finalidad originaria. Para esto debe ser la complicada y precavida técnica inglesa de la ley, la disolución en una múltiple casuística, la acumulación de expresiones sinónimas, las definiciones, hasta donde sea posible, de las palabras usadas en la ley; una técnica legal de un género sumamente pesado y desafortunado. Pero el punto de vista de la elegancia iuris, la tendencia injustificada a ver lo mejor en lo que es sencillo y estéticamente bello, no tiene en Inglaterra la misma fuerza sobre los espíritus que en la jurisprudencia continental" (pp.48-49) Conf. RADBRUCH, GUSTAV: "El espíritu del Derecho Inglés", traducción de Fernando Vela, Revista de Occidente, 1958, p. 118³.

³ Cita del Excmo. Sr. D. Antonio RODRÍGUEZ ADRADOS, Comunicación discutida del Pleno de Académicos de Número de la Real Academia de Jurisprudencia y Legislación, el día 5 de junio de 2000.

CONCEPTO DE DOCUMENTO.

Nuestra legislación procesal, inspirada en el pensamiento del profesor Devis Echandía, quien coincidía en esta materia con la concepción de Carnelutti, acogió la teoría de la representación la cual fue consagrada en el artículo 251 del estatuto procesal civil, en los siguientes términos:

“Art. 251. 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 carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares”.

Recordemos que el ilustre maestro italiano lo definió, así: “El documento no es solo una cosa, sino una cosa representativa, o sea capaz de representar un hecho”⁴.

El Profesor Devis Echandía por su parte lo definió, así: “Documento es toda cosa que sirve de prueba histórica indirecta y representativa de un hecho cualquiera”⁵.

El Profesor Parra Quijano, quien glosa la definición del maestro Devis, lo define así:

“Documento es todo objeto producido, directa o indirectamente, por la actividad del hombre y que, representa una cosa, hecho o una manifestación del pensamiento”⁶.

Atendiendo estas definiciones podemos afirmar que el documento electrónico en esencia reúne las mismas características. De ahí que este tema debe ser abordado con la legislación procesal existente y, perfectamente, haciendo una interpretación analógica y atendiendo las definiciones contenidas en la ley, esto es, mediante este complemento interpretativo de orden gramatical y semántico. En estas condiciones

⁴ PARRA Quijano Jairo, Tratado de La Prueba Judicial, Los Documentos, Tomo III, Ediciones Librería del Profesional, Primera Edición 1987, p. 4.

⁵ PARRA Quijano Jairo, ob. cit., p. 12.

⁶ PARRA Quijano, Jairo, ob. cit. p. 13.

nuestros jueces y abogados pueden asumir la interpretación adecuada del mismo frente a los casos concretos.

No en vano ya lo han hecho con anterioridad atendiendo medios similares como: las grabaciones magnetofónicas, las radiografías, los discos de todas las especies, las cintas cinematográficas, etcétera, han sido mencionadas como especies de documentos en el artículo 251 del Código de Procedimiento Civil.

Su aplicación directa está en la regulación que del comercio electrónico ha hecho la ley la cual toma como ejemplo la información contenida en el intercambio electrónico de datos (EDI), internet, correo electrónico, telegrama, télex o telefax, contabilidad en medios magnéticos etcétera. (Ver además estatuto y reglamentos de la ley estatutaria de la Administración de Justicia).

EL DOCUMENTO ELECTRÓNICO.

Para formar una noción de lo que debemos considerar como documento electrónico partimos de la consideración general del concepto de documento para aproximarnos a una definición, así: Todo objeto representativo o declarativo, testimonial o dispositivo, producido por el hombre de manera directa o indirecta, contenido en un soporte electrónico, decodificable mediante las máquinas y procedimientos informáticos correspondientes.

Angelo Gallizia citado por Ernesto Rengifo García en su ponencia "El Documento Electrónico"⁷ lo define de la siguiente manera: "Es un objeto físico dirigido a conservar y transmitir informaciones mediante mensajes en lenguaje natural, realizado con la intermediación de funciones electrónicas".

Notemos que el documento electrónico al igual que el documento en soporte de papel tiene los siguientes elementos comunes esenciales:

- a) Un corpus que es su elemento declarativo, (testimonial o dispositivo), o representativo, esto es, el contenido del soporte: disco duro, disco flexible, memoria del computador, cinta del casete etcétera;

- b) Una grafía. Así como la escritura de un idioma implica la existencia de letras en su texto, en el documento electrónico éstas están dadas por los caracteres electromagnéticos o el denominado lenguaje de máquina. Como lo anota el profesor Jairo Parra: "En ocasiones es menester acudir a una suerte de "traducción", cuando el documento se encuentra redactado en "lenguaje de máquina"; es lo mismo que ocurre cuando se ha plasmado en idioma extranjero"⁸.
- c) Un elemento intelectual, el cual está dado en ambos casos, documento escrito y documento electrónico, por la capacidad creativa del intelecto humano de manera directa o indirecta. Directa cuando el mismo elabora el documento, indirecta cuando programa una máquina para que lo elabore siguiendo las pautas de su programación.

La diferencia, como podemos apreciarlo está en que para recibir la información en él contenida se hace necesario utilizar herramientas informáticas, esto es, una máquina y unos procedimientos (Hardware y software) para que traduzcan a nuestro lenguaje natural el lenguaje del documento electrónico que está elaborado en forma digital, a través de un sistema alfanumérico.

FINALIDAD PROBATORIA.

Al igual que los otros medios de prueba, el documento electrónico tiene como finalidad procesal y probatoria fundar el juicio de certeza sobre las alegaciones fácticas de las partes, tal cual lo impone el artículo 177 del C. de P. C. Por tanto, se hace necesario que sea auténtico o pueda establecerse su autenticidad, esto es, como lo exige la ley procesal nuestra, debe existir certeza sobre la persona que lo ha elaborado.

Autenticidad del documento electrónico.

La autenticidad del documento electrónico puede establecerse por cualquiera de los medios establecidos en el C. de P. C., o conforme a las disposiciones de la Ley 527 o ley de comercio electrónico y sus reglamentaciones.

⁸ PARRA Quijano, Jairo, ob.cit. p. 20.

La Ley 527 de 1999 dispone de varios elementos plenamente definidos para construir la noción de documento, su autenticidad, su eficacia y valor probatorio. Debemos por tanto, ponerlos de presente y traer sus definiciones para establecer plenamente las reglas de juego. Igualmente debemos compararlas con las de otros países para establecer el punto en que nos encontramos al respecto, las diferencias, ventajas o desventajas.

El Mensaje de Datos.

El contenido del documento está dado por el mensaje de datos, el cual tiene un carácter representativo o declarativo y, éste, una declaración testimonial o dispositiva. Es tan importante la noción de mensaje de datos que algunos, como el honorable magistrado de la Corte Suprema de Justicia Luis Fernando Ramírez, en reciente conferencia en el seno del Instituto Colombiano de Derecho Procesal, han sostenido que: "documento electrónico, es el mensaje de datos".

La ley lo define así:

Artículo 2º. Definiciones. Para los efectos de la presente ley se entenderá por:

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

Hay que destacar además, que el documento electrónico o mensaje de datos adquiere fuerza probatoria por mandato legal conforme a la Ley 527, en los siguientes términos:

Artículo 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 en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil. (Subrayas nuestras).

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y, probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de

un mensaje de datos o en razón de no haber sido presentado en su forma original.

Sobre el particular es relevante analizar las precisiones hechas por la Corte Constitucional en la sentencia C-662-00, así: "La noción de 'mensaje' comprende la información obtenida por medios análogos en el ámbito de las técnicas de comunicación modernas, bajo la configuración de los progresos técnicos que tengan contenido jurídico.

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

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

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 para los fines contables, impositivos y reglamentarios; afirma derechos y obligaciones jurídicas entre los intervinientes y es accesible para su ulterior consulta, es decir, que la información en forma de datos computarizados es susceptible de leerse e interpretarse.

Por otra parte, en el proyecto de ley se hace hincapié como condición de singular trascendencia, en la integridad de la información para su originalidad y establece reglas que deberán tenerse en cuenta al apreciar esa integridad, en otras palabras que los mensajes no sean alterados y esta condición la satisfacen los sistemas de protección de la información, como la Criptografía y las firmas digitales, al igual que la actividad de las Entidades de Certificación, encargadas de proteger la información en diversas etapas de la transacción, dentro del marco de la autonomía de la voluntad.

Así mismo, cuando el contenido de un mensaje de datos sea completo y esté alterado, pero exista algún anexo inserto, éste no afectará su

condición de "original". Esas condiciones se considerarían escritos complementarios o serían asimiladas al sobre utilizado para enviar ese documento "original".

- Equivalentes funcionales

El proyecto de ley, al igual de la Ley Modelo, sigue el criterio de los 'equivalentes funcionales' que se fundamenta en un análisis de los propósitos y funciones de la exigencia tradicional del documento sobre papel, para determinar cómo podrían cumplirse esos propósitos y funciones con técnicas electrónicas.

Se adoptó el criterio flexible de "equivalente funcional", que tuviera en cuenta los requisitos de forma fiabilidad, inalterabilidad y rastreabilidad, que son aplicables a la documentación consignada sobre papel, ya que los mensajes de datos por su naturaleza, no equivalen en estricto sentido a un documento consignado en papel.

En conclusión, los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la ley⁹.

Su Autenticidad

Al igual que en los documentos soportados en papel el documento electrónico requiere del elemento Autenticidad. Por consiguiente debemos establecer su autoría. La ley nuestra al igual que las leyes de otros países al igual que la legislación de la ONU y de la Comunidad Económica Europea, así como la doctrina y la jurisprudencia universales establecen, en punto del documento electrónico, que la autoría del documento está dada con mayor o menor certeza por la presencia de la denominada firma digital o firma digital avanzada y su correspondiente certificación.

Notemos que nuestra legislación no regula, para el caso del documento soportado en papel, lo relativo a la firma. Sobre el particular Lessona apunta

⁹ Corte Constitucional Sentencia C-662-00.

que es laudable que la ley no regule el punto pues ello se ajusta al espíritu antiformalista del derecho moderno y agrega: "Lo que la ley pide es la expresión de la identidad de la persona y de la letra; el juez es quien en cada caso debe aseverarla. Así, por ejemplo, si el nombre y apellido constituyen la firma por excelencia, no hay nada que oponer en el caso en que una firma conste sólo de la inicial del nombre y del apellido incompleto, o bien cuando conste sólo de la inicial del nombre y el apellido completo, o bien cuando conste del apellido o aún del nombre tan solo; como en los casos de los soberanos, papas, obispos. El apellido propio podrá ser sustituido por un seudónimo usual, por el nombre usado en religión o en la vida artística; la mujer casada firmará válidamente con el apellido del marido añadido al suyo. Los errores ortográficos que no hagan incierta la firma no la invalidan. La firma debe ser obra personal del firmante".

Recordemos con ANTONIO RODRÍGUEZ ADRADOS que: "la función primordial de la firma no es esa identificación del firmante, sino la de ser instrumento de su declaración de voluntad.

La verdadera función de la firma es, en efecto, la función declarativa, que es la que exige esa actuación personal del signante —enmascarada bajo el requisito de la manuscritura— imponiendo al documento una grafía. Una firma declara muchas cosas; declara que aquello es un documento, y no un proyecto o borrador, puesto que no hay documento sin autor; declara al ser suscripción que el documento está terminado, a la manera de la completo de los tabeliones bizantinos; declara que el firmante asume como propio el documento, y lo aprueba y confirma, en el concepto (otorgante, testigo, etc.), y en la medida que el mismo documento establece. Pero la firma no se limita al documento, pues lo que principalmente se firma es su contenido, las manifestaciones o declaraciones que el firmante efectúa mediante el documento, y por tanto en los documentos negociales su declaración de voluntad"¹⁰.

Precisamente para evitar cometer errores de orden interpretativo nuestra ley al igual que las legislaciones existentes en otros países sobre la materia, ha definido lo que ha de entenderse por firma digital, así:

- d) Firma digital.** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático

¹⁰ RODRÍGUEZ ADRADOS, Antonio, conf. Citada, p. 28.

conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

La ley de Comercio electrónico igualmente regula los atributos de la firma digital y la equipara a la firma manuscrita si cumple los requisitos que ella establece, así:

PARTE III

FIRMAS DIGITALES, CERTIFICADOS Y ENTIDADES DE CERTIFICACIÓN

CAPÍTULO I

Firmas digitales

Artículo 28. Atributos jurídicos de una firma cierta. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquélla tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

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

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

Igualmente la ley regula la eficacia de la firma digital en todos aquellos eventos en que se exige como requisito la existencia de una firma en el documento electrónico, esto es, en el mensaje de datos.

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

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

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

Al analizar las dos disposiciones podremos concluir con la ayuda de los conceptos que transcribiremos adelante que el artículo 28 se asimila a la denominada firma digital avanzada y el artículo 7 a la denominada simplemente firma digital.

La Corte Constitucional precisa el concepto técnico de firma digital en los siguiente términos: "Una de las formas para dar seguridad a la validez en la creación y verificación de una firma digital es la Criptografía, la cual es una rama de las matemáticas aplicadas que se ocupa de transformar, mediante un procedimiento sencillo, mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.

Mediante el uso de un equipo físico especial, los operadores crean un par de códigos matemáticos, a saber: una clave secreta o privada, conocida únicamente por su autor, y una clave pública, conocida como del público. La firma digital es el resultado de la combinación de un código matemático creado por el iniciador para garantizar la singularidad de un mensaje en particular, que separa el mensaje de la firma digital y la integridad del mismo con la identidad de su autor".

Para enriquecer los conceptos de la Corte Constitucional sobre la criptología podemos agregar lo siguiente:

Empecemos por preguntarnos ¿Qué es la criptografía en su noción más elemental? Respondamos con el Diccionario Enciclopédico de Derecho Usual diciendo: "Arte de escribir en forma enigmática o ininteligible para quien no posea la clave empleada.

1. Protagonistas. A quien cultiva esta ciencia y arte, al que prepara claves y códigos que ofrezcan cierta garantía de seguridad, se le

llama criptólogo; y descryptador, al mismo criptólogo cuando aplica sus conocimientos especiales al descubrimiento de los métodos empleados en un escrito cifrado, para descifrarlo. Los que mecánicamente aplican las claves facilitadas por el criptólogo para cifrar un texto normal, o al revés, se llaman cifradores o descifradores, respectivamente.

2. Procedimientos. Los sistemas empleados en criptografía son el de sustitución y el de transposición. De ellos nace una gama muy variada de métodos. El primero consiste en reemplazar las letras o grupos de letras por otros signos; el segundo se basa en colocar las mismas letras del texto normal en orden distinto y, al parecer, en forma arbitraria, pero con sujeción claro está, a la clave determinada. La diplomacia durante la paz, en campaña los ejércitos y siempre los servicios especiales recurren a la criptografía para encubrir sus mensajes reservados, o los que pretenden pasar por tales.

“La criptología moderna, es decir la que se ha desarrollado a partir de 1976, es la tecnología que hace posible implementar las medidas de seguridad necesarias para crear la confianza en la infraestructura Global de la Información.

Por criptología podemos entender como aquella ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones, e inversamente la obtención de la información protegida. Abarca por tanto la criptografía (textos, imágenes y datos), criptografía (voz) y al criptoanálisis.

Existen multitud de tipos de encriptación. La aplicación de uno o de otro lo dirá la práctica comercial pues dependiendo de su efectividad serán más o menos utilizados. La gran seguridad que actualmente existe en el tema de la encriptación ha llegado al punto que en Estados Unidos estos métodos se consideran armas de guerra y por tanto se prohíbe su exportación a otros países. El motivo es claro y evidente, pues si cae en otras manos con no muy buenas intenciones, la delincuencia ganaría muchos enteros, pues la posibilidad de pasar desapercibidos ante el gobierno USA con la utilización de una de estas técnicas sería patente, lo cual nos lleva a apreciar las mencionadas técnicas y de esta forma a confiar en la seguridad del comercio electrónico paso clave para su eclosión en la red de redes, es decir, en Internet”.

TIPOS DE ENCRIPCIÓN.

- a) Encriptación mediante claves simétricas. Este tipo de encriptación supone una clave, conocida por todas las partes, para poder decodificar la información, o sea, para poder desencriptarla. El problema radica, como es obvio, en ello, ya que al todas las partes conocer la clave cualquiera de ellas puede modificar o destruir el mensaje.
- b) Encriptación mediante claves asimétricas o públicas. Existen también sistemas simétricos de cifrado. Cada usuario dispone de dos claves una pública, que debe revelar o publicar para que los demás puedan comunicarse con él y una privada que debe mantener en secreto. Cuando un usuario desea mandar un mensaje protegido, cifra el mensaje con la clave pública del destinatario. De esta manera, sólo el destinatario puede descifrar con su clave secreta el mensaje cifrado. Ni siquiera el emisor del mensaje puede descifrar el mensaje cifrado por él. Estos mensajes responden a la necesidad de comunicación en redes muy grandes, donde la gestión de claves secretas es inviable, pero además, y esta es la gran revolución de la criptografía moderna, solucionan los problemas de autenticación de emisor y receptor, proporcionan la posibilidad de firmar digitalmente los mensajes y garantizan el contenido de los mismos. No obstante adolecen de un punto débil: ¿Cómo se asocian pares de clave pública-clave privada correctos en sí mismos con personas físicas? La solución la aportan las entidades de certificación (notarios electrónicos) que son entes fiables y altamente reconocidos que firman, con conocimiento de causa y asunción de responsabilidad, las claves públicas de las personas rubricando con su firma su identidad.
- c) Encriptación mediante códigos de integridad. En este sistema se utilizan funciones matemáticas que derivan de una huella digital a partir de un cierto volumen de datos. (Una huella tiene de 128 a 160 bits). Es teóricamente posible encontrar dos mensajes con idéntica huella digital, pero la probabilidad es ínfima. Si se *manipulan los datos la huella cambia y modificar la huella de forma tan sabia para obtener la misma huella es algo computacionalmente inabordable en un plazo razonable.*
- d) Encriptación mediante firma digital. Dado un mensaje, basta calcular su huella digital y cifrarla con la clave secreta del

remite para obtener simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser (autenticación). Las firmas digitales suelen ir asociadas a una fecha. La fecha de emisión y posiblemente la fecha de vencimiento de validez suelen proporcionarse en texto claro e incorporarse al cálculo de la huella digital para ligarlas irremediamente.

FUNCIONES DE LA FIRMA DIGITAL

La firma digital debe cumplir idénticas funciones que una firma en las comunicaciones consignadas en papel. En tal virtud, se toman en consideración las siguientes funciones de esta:

- 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.

Como quiera que la autenticidad del documento electrónico está dada, entre otras reglas de apreciación, por el concepto de firma electrónica de la cual como anticipamos hay dos especies: la de firma digital simple y la de firma digital avanzada, nos detendremos a reflexionar sobre el punto con el objeto de profundizar en el tema con la ayuda de otras legislaciones y de tratadistas del viejo continente, los cuales nos enseñarán que el concepto de firma electrónica no puede unificarse debido a las diferencias tecnológicas existentes.

España: real Decreto-ley 14/1999 art. 2.a): "Firma electrónica. Es el conjunto de datos, en forma electrónica, anejos¹¹ a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio de identificar formalmente al autor o a los autores del documento que la recoge".

Ibíd. 2.b) "Firma electrónica avanzada. Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que

¹¹ DICCIONARIO DE LA LENGUA ESPAÑOLA, REAL ACADEMIA ESPAÑOLA, Vigésima Primera edición. 1. (Del Latín *annexus*, añadido) 1. Adj. Unido o agregado a otra persona o cosa, con dependencia, proximidad y estrecha relación respecto a ella. 2. Propio, inherente, concerniente.

éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior a estos”.

La firma electrónica avanzada en opinión de los expertos es la que garantiza los dos extremos del documento: la identificación del firmante y la integridad del mensaje cosa que una firma electrónica no puede asegurar.

Sobre el particular RODRÍGUEZ ADRADOS expresa que: En el estado actual de la técnica informática y en el mercado tiene, por el contrario, absoluto predominio, por su mayor fiabilidad el sistema de pareja asimétrica de claves para la codificación y ulterior descodificación de los mensajes. Un sistema simétrico, en el que una misma clave sirve para codificar el mensaje y para descodificarlo, sólo resulta adaptado a las redes cerradas, en que se puede proporcionar la clave al destinatario, si es que no se le había dado antes a conocer; pero una y otra cosa son bien arriesgadas en redes abiertas. En el sistema asimétrico, como bien es sabido, cada usuario tiene dos claves, una clave privada, que sólo él conoce, y una clave pública, destinada a ser conocida por los destinatarios de los mensajes, ambas claves están íntimamente entrelazadas, de manera que el mensaje cifrado con una de ellas, sólo podrá ser descifrado por la clave pareja de la misma persona. Aplicado tal procedimiento a la firma de un texto, éste en su totalidad o, en la práctica dominante, un resumen del mismo o abstract, se encripta por el emisor del mensaje (en nuestro caso por el oferente, o por una de las partes de un contrato) mediante su propia clave privada; y en consecuencia, podrá descifrarse mediante la clave pública del mismo emisor (del mismo oferente o del mismo contratante)¹².

Las leyes alemana e italiana atendiendo la realidad tecnológica se refieren al procedimiento de claves asimétricas, privada y pública. Estas leyes no hablan de firma digital avanzada pero dejan fuera del sistema aquellas firmas digitales originadas en otros sistemas o procedimientos menos avanzados y, por tanto, menos confiables tecnológicamente hablando, (caso de Alemania) o les reconocen menores efectos (legislación italiana).

Alemania: Art. 2. (1) “Una firma digital, en el contexto de esta ley, es un sello de datos digitales creado con una llave privada, que permite

¹² RODRÍGUEZ ADRADOS Antonio, Conf. Cit. P. 17-18.

determinar el propietario de la firma y la ausencia de adulteración de los datos, a través de la llave pública asociada a la anterior y determinada en un certificado”.

Italia, artículo 1 “... se entiende: ... b) por firma digital, el resultado del procedimiento informático (validación), basado sobre un sistema de bases asimétricas en pareja, una pública y otra privada, que respectivamente permiten al suscriptor, por medio de la clave privada, y al destinatario, por medio de la clave pública hacer manifiesta y verificar la providencia e integridad de un documento informático o de un conjunto de documentos informáticos”.

Francia: art. 1364.4, párrafo 2.: “Cuando (la firma) es electrónica, consiste en el uso de un procedimiento fiable de identificación que garantice su nexa con el documento que se agrega”. La fiabilidad se presume cuando “la firma electrónica es creada, la identidad del firmante asegurada y la integridad del documento garantizada en las condiciones fijadas por el decreto en Consejo de Estado”.

La noción de firma digital en Colombia, acoge los más avanzados conceptos técnicos que garantizan la seguridad del mensaje y permiten tanto la identificación del sujeto (certeza sobre el origen) como la integridad original del mismo.

Para ilustrar con un ejemplo la noción de firma digital avanzada traemos como ejemplo el puesto en documento de la Cámara de Comercio de Medellín¹³:

En el proceso de emisión de un certificado digital, se crean dos llaves o claves en forma simultánea: una privada y una pública. La llave pública es de conocimiento general y forma parte del certificado digital que será emitido por la entidad y utilizada por el suscriptor para identificarse en Internet. La clave privada, por el contrario, es almacenada en la computadora del solicitante del certificado y es manejada exclusivamente por este. Los estándares de seguridad exigen que nadie diferente, ni siquiera la autoridad certificante, puedan tener acceso a esta clave privada.

¹³ CÁMARA DE COMERCIO DE MEDELLÍN. COMERCIO ELECTRÓNICO – IMPLICACIONES JURÍDICAS, p. 5.

Una vez el mensaje llega a su destinatario, este certifica cuál es el origen del mensaje. La verificación se hace mediante el certificado del creador u originador, el cual contiene el nombre y la llave pública del mismo. Si dicha llave pública logra el efecto de descriptar o permitir la lectura de la firma contenida en el mensaje, puede tener la seguridad de que éste efectivamente fue creado mediante el uso de la llave privada correspondiente.

Examinados los conceptos y las notas doctrinarias traídas en comento, debemos concluir con la Corte Constitucional nuestra así:

“..., 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 tradicionalmente asegurados por la firma autógrafa, por lo que se crea la necesidad de que existan establecimientos que certifiquen la validez de esas firmas.

Por lo tanto, quien realiza la verificación debe tener acceso a la clave pública y adquirir la seguridad que el mensaje de datos que viene encriptado corresponde a la clave principal del firmante; son las llamadas entidades de certificación que trataremos más adelante”.

Entidades de certificación

d) Entidad de Certificación. Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;

Sobre las Entidades de certificación, al analizar su naturaleza, la función que cumplen, el ejercicio de inspección sobre las mismas y otros temas relacionados con ellas, ha establecido doctrinariamente la Corte Constitucional en la Sentencia 662-00, fundamento de este escrito, lo siguiente:

“La entidad de certificación, expide actos denominados 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, para lo cual vale la pena detenerse un momento.

El artículo 365 de la Constitución Política hace referencia al tema de los servicios públicos, los cuales pueden ser prestados tanto por las entidades públicas como las privadas o conjuntamente. Esta norma permite que este servicio lo presten los particulares, si reúnen los requisitos exigidos por la ley y cuenta con la aprobación de la Superintendencia, organismo rector para todos los efectos.

El proyecto de ley señala que podrán ser entidades de certificación, las Cámaras de Comercio y en general las personas jurídicas, tanto públicas como privadas, autorizadas por la Superintendencia respectiva, que cumplan con los requerimientos y condiciones establecidos por el Gobierno Nacional, con fundamento en el artículo 31 del proyecto.

Una vez las entidades de certificación sean autorizadas, podrán realizar actividades tales como, emitir certificados en relación con las firmas digitales; ofrecer o facilitar los servicios de creación de firmas digitales certificadas; servicios de registro y estampado cronológico en la transmisión y recepción de mensajes de datos; servicios de archivo y conservación de mensajes de datos, entre otras.

A la par con las actividades definidas anteriormente, estas entidades tendrán deberes que cumplir frente a los involucrados dentro del proceso mercantil, deberes atinentes a cada una de las actividades que pretendan ejercer.

En consecuencia, las entidades de certificación, son las encargadas entre otras cosas, de facilitar y garantizar las transacciones comerciales por medios electrónicos o medios diferentes a los estipulados en papel e implican un alto grado de confiabilidad, lo que las hace importantes y merecedoras de un control ejercido por un ente público, control que redundará en beneficio de la seguridad jurídica del comercio electrónico.

La comisión redactora del proyecto de ley, consideró que la Superintendencia de Industria y Comercio debe ser la entidad encargada del control y vigilancia de las entidades de certificación, por cuanto su competencia es afín con estas labores.

La función que actualmente ejercen las Superintendencias y que les fue delegada, le corresponde constitucionalmente al Presidente de la República como Suprema Autoridad Administrativa, cuando señala que una de sus funciones es la de ejercer la inspección y vigilancia de la prestación de los servicios públicos.

En razón a que la naturaleza de las funciones de las entidades de certificación se consideran como la prestación de un servicio público, la inspección y vigilancia de los servicios públicos que tienen que ver con la certificación, actividades que ejercerán las entidades de certificación, debe radicarse en cabeza de una Superintendencia como la de Industria y Comercio”.

De la doctrina de la Corte, de la ley y de la doctrina extranjera –en cuanto aplicable a nuestro caso– podemos concluir sobre el particular:

- Las entidades de certificación tienen por objeto certificar las claves públicas para determinar la autoría del mensaje de datos y prestar otros servicios como el intercambio de mensajes mediante sistemas confiables en los términos del Decreto Reglamentario 1747/2000.
- Este servicio puede ser prestado por personas jurídicas públicas o privadas, nacionales o extranjeras.
- Las entidades de certificación no son autoridades, ni guardadoras de la fe pública y, en consecuencia, no pueden dar fe de la firma puesta en un documento ni autorizar la elevación de un documento electrónico a la categoría de público, como por ejemplo una minuta de escritura firmada digitalmente por los contratantes. Esto solamente podrán hacerlo los notarios que sean autorizados como entidad de certificación en el momento en que reciban esta autorización por parte del Ente Administrativo en los términos de la Ley 588 de 2000.

La legislación española tiene prohibición expresa sobre el particular en los siguientes términos:

Decreto ley 14/1999 artículo 1.2.1 “Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este real decreto-ley no sustituyen ni modifican las que regulan las funciones que corresponde

realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos”.

En este sentido creemos que nuestra legislación abre grandes posibilidades pues en su artículo primero ha hecho sólo dos salvedades a la información por este medio:

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

En nuestra opinión el legislador colombiano ha abierto la posibilidad de que el documento informático se transforme en escritura pública, conforme al contenido de los artículos 6°, 7° y 8° de la Ley 527/99 y de la Ley 588/2000 artículos primero y noveno.

A pesar de esa opinión bien vale tener en cuenta las voces de otras latitudes sobre el particular.

“La escritura pública informática

La ley francesa del año 2000 ha introducido en el derecho positivo del país vecino como forma y como prueba el instrumento público negocial informático, en la terminología española escritura pública informática, que ha dejado de ser por tanto, una mera elucubración doctrinal. Algo habrá, pues, que decir de ella, aunque quizá no pase de elucubración legal y nuestro derecho la excluya en el artículo 1.2.1 del Real decreto-ley 14 de 1999.

... (Ver disposición transcrita infra).

Recordemos que el reglamento italiano tampoco acepta esa variedad instrumental pues se detiene según acabamos de ver en la autenticación notarial de la firma digital, extendida por el Notario en Documento papel.

El problema que planteamos es totalmente distinto al de la posibilidad de que los notarios actúen como prestadores de servicios de certificación de firmas electrónicas.

Prontamente se había llegado a la convicción de que el documento informático no podía funcionar de manera autónoma; que no bastaba con que el destinatario comprobase en una guía, a la manera de las de teléfonos, quién era el titular de la clave pública, sino se precisaba la intervención de un tercero de confianza de las partes, con carácter de verdadera autoridad de certificación, para identificar a ese titular, comprobar sus facultades si intervenía en representación de otra persona y acreditar la vigencia de la certificación.

Estas misiones no podían ser asumidas por el llamado notary public norteamericano, lego en derecho, por lo que en los Estados Unidos, surgió la idea de perfeccionarle creando el que no con demasiado acierto se denominó cibernotario; y, en los países de derecho latino se pensó, con evidente precipitación, que eran los mismos notarios latinos los que debían desempeñar el papel de autoridades de certificación; la "figura del notario latino –dice Mario Miccoli–, difícilmente se lograría compendiar más felizmente y más sucintamente que indicándole como un sujeto de confianza de la sociedad dotado de terceraidad y poderes de certificación, indicando por tanto los elementos que según la opinión prevalente deben ser propios de la Certificación Authority"¹⁴, con lo cual MICCOLI, nada menos que presidente de la Comisión de Seguridad Jurídica e Informática de la Unión Internacional del Notariado Latino, se olvidaba de que Autoridad de Certificación y Notario en manera alguna se identifican aunque tengan algunas tareas comunes. El Notario tiene otras funciones más amplias, de determinación de la voluntad de los otorgantes, información y consejo, redacción y adecuación, ajenas totalmente a esas Autoridades de Certificación nacidas –no puede olvidarse– en el ámbito del Derecho Norteamericano. Pero la Autoridad de Certificación tiene también funciones que actualmente no competen al notario latino, algunas de las cuales, quizá, no les sea posible asumir.

Toda prudencia es poca a la hora de introducir en el derecho positivo un instrumento público negocial informático; es preferible dejar que el tiempo madure las sensibilidades y muestre los resultados favorables o desfavorables que se produzcan en otros ámbitos, puesto que como escribí

¹⁴ Conf. MICCOLI, Mario: "Comercio Telemático: Una Nuova realta 'nel campo del diritto". <http://www.notariato.it/forum/rbogot.hotm> p. 7 de 12, respectivamente, 27-11-1997.

LISERRE, los notarios están "mayormente expuestos como categoría, a los riesgos y a las incertidumbres de una innovación que incide centralmente en su función de productores, por así decir, de autenticidad"¹⁵.

Aportación del documento electrónico al proceso

Oportunidad. Atendiendo lo dispuesto en el artículo 10 de la Ley 527/ 99 la oportunidad probatoria del documento electrónico está dada por la normas del C. de P.C. A continuación transcribimos las normas correspondientes:

"Artículo 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 en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y, probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original".

Código de Procedimiento Civil.

"Artículo 183.- Para que sean apreciadas por el juez las pruebas deberán solicitarse, practicarse e incorporarse al proceso dentro de los términos y oportunidades señalados para ello en este código.

Si se trata de prueba documental o anticipada también se apreciarán las que se acompañen a los escritos de demanda o de excepciones o a sus respectivas contestaciones, o a aquellos en que se pomuevan incidentes o se les dé respuesta. El juez resolverá expresamente sobre la admisión de dichas pruebas, cuando decida la solicitud de las que pidan las partes en el proceso o incidente.

Cuando el proceso haya pasado al despacho del juez para sentencia, las pruebas practicadas por comisionado que lleguen posteriormente,

¹⁵ LISERRE, Antonio: "L' avvento del documento elettronico". Rivista di Diritto Civile, sep-
oct 1998, p. 475-82; las palabras citadas en p. 481.

serán tenidas en cuenta para la decisión, siempre que se hubieren cumplido los requisitos legales para su práctica y contradicción. En caso contrario, y cuando en la misma oportunidad llegaren pruebas documentales cuyos originales o copias se hayan solicitado a otras oficinas, el juez de primera instancia no las tendrá en cuenta, pero serán consideradas por el superior. Este de oficio o a petición de parte, ordenará el trámite que falte a dichas pruebas. Si se trata de documentos, la parte contraria a la que los adujo podrá tacharlos de falsos dentro del término de ejecutoria del auto que admita la apelación”.

Debe considerarse igualmente la posibilidad adicional establecida por el artículo 184 ibídem:

“Artículo 184. Si se han dejado de practicar pruebas sin culpa de la parte que las pidió, el término señalado para tal efecto se ampliará a petición de aquélla, hasta por otro igual que se contará a partir de la notificación del auto que así lo disponga.

Vencido el término probatorio o el adicional en su caso precluirá la oportunidad para practicar pruebas y el juez deberá, so pena de incurrir en la falta disciplinaria respectiva, disponer sin tardanza el trámite que corresponda”.

Forma de aportarlo. Las partes deben aportar los objetos o medios instrumentales contentivos del documento electrónico que permitan la traducción del lenguaje digital al lenguaje ordinario comprensible para el juez y para los sujetos procesales. Si para el efecto fuere necesario dictámenes u otros medios de prueba corresponderá a la parte que proponga el documento electrónico como prueba, pedirlos oportunamente.

Específicamente el artículo 6°, inciso primero de la Ley 527 dispone:

*“Artículo 6°. Escrito. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, **si la información que éste contiene es accesible para su posterior consulta**”.* (Subrayas nuestras).

El concepto de **original** está definido en los siguientes términos:

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

- a) *Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;*
- b) *De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar”.*

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

Por lo demás, en cuanto a su práctica rigen las reglas generales de publicidad y contradicción de la prueba, tacha de falsedad del documento y consideramos indispensable en este tipo de prueba, cuando la información se va a decodificar de su encriptamiento y a convertir al lenguaje corriente, la presencia del juez en el procedimiento.

Si la prueba debe practicarse como prueba anticipada deberá hacerse con la comparecencia de la parte contra quien se va a utilizar en el proceso.

Eficacia y valor probatorio del documento electrónico. La Ley 527/99 traza unas pautas sobre el criterio para valorar este tipo de prueba en los siguientes términos:

*“Artículo 11. Criterio para valorar probatoriamente un mensaje de datos. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. **Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en 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”.** (Subrayas nuestras).*

Además de los criterios fijados por la ley debemos resaltar que para que el soporte electrónico adquiera la misma fuerza que el soporte de papel se deben cumplir tres condiciones fundamentales:

- a) **Identificación del autor del documento.** Esta se hace confrontando la firma electrónica o por cualquier otro medio probatorio, incluidas las presunciones establecidas en la ley (Arts: 17, 19, 21, etc.).
- b) **El proceso de generación del documento debe garantizar su integridad.** Es importante y definitivo para tenerlo como medio de prueba poder establecer que el documento se generó por la voluntad de su autor, de manera directa o por instrucciones o autorización suyas, y que está conforme a ellas.
- c) **Garantizar la integridad del documento.** Recordemos que el concepto de original, en los términos de esta ley exige la garantía confiable de que se ha conservado el documento en su integridad, a partir del momento en que se generó por primera vez en su forma definitiva; y, de la disponibilidad para presentar dicha información a la parte o a cualquier persona que por motivos judiciales la desee confrontar.

En este aspecto sintetizamos lo expuesto por la Corte Constitucional en la Sentencia 662-00, así: "Al hacer referencia a la definición de documentos del Código de Procedimiento Civil, 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 algunos criterios como: confiabilidad, integridad de la información e identificación del autor.

Criterio para valorar probatoriamente un mensaje de datos. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la confiabilidad de la forma en la 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 (artículo 11)".

" Los medios tecnológicos actuales permiten generar documentos que cumplen con todas las condiciones indicadas. Los medios que proporciona la criptografía –entre ellos especialmente la firma digital– están hoy en día al alcance de cualquier comercio o empresa y, gracias a ellos pueden emitirse los documentos que cumplen con todos los requisitos de la nueva legislación. Tómese en consideración que, paralelamente a esta norma,

deben emitirse normas sobre firma electrónica a efectos de permitir la identificación de los firmantes-autores de los documentos así como la integridad de estos últimos. Es indisoluble en tal sentido, el tratamiento normativo de uno y otro elemento"¹⁶.

Por último, en los términos de la ley de comercio electrónico y del Código de Procedimiento Civil los documentos electrónicos tendrán el valor probatorio que le asignan las normas procesales. Así por ejemplo: si el documento electrónico no está firmado por la parte a quien se opone, en los términos del artículo 269 C. de P. C. "... sólo tendrán valor si fueren aceptados por ella o sus causahabientes".

¹⁶ Ministerio de Justicia de España. Las nuevas tecnologías en las normas procesales. El documento electrónico como medio de prueba. Procedimiento probatorio de los documentos electrónicos. Madrid, 21 de julio de 2000.