FIRMA DIGITAL – Certificación / CERTIFICACIÓN DE FIRMA DIGITAL – Parámetros / ENTIDAD DE CERTIFICACIÓN – Funciones / CERTIFICADO EXPEDIDO POR ENTIDAD DE CERTIFICACIÓN CERRADA – Efectos / CERTIFICADO EXPEDIDO POR ENTIDAD DE CERTIFICACIÓN ABIERTA – Efectos / MENSAJE DE DATOS – Validez

En cuanto a la alegada vulneración del literal c) del artículo 2º de la Ley 527, que define a la firma digital, la Sala no observa tal violación, pues, por un lado, la Entidad de Certificación Abierta al transmitir la referida firma digital debía cumplir las exigencias establecidas para tenerla como tal, ya que estaba obligada a someterse a las directrices previstas en el artículo 28 de la Ley 527 que determinó sus atributos; y por el otro, comoquiera que los datos difundidos por la Entidad de Certificación Cerrada no se constituían en una firma digital, al disponer la norma acusada que dichas entidades debían indicar expresamente que los mensajes por estas transmitidos no producirían los efectos de la citada firma, se salvaguardó la norma que la definió, toda vez que para ser emitida, la entidad debía estar autorizada y además, debía atenerse a las propiedades exigidas por la Ley en mención. De igual forma, no se encontró que las normas censuradas vulneraran el reconocimiento jurídico de los mensajes de datos, ni la información requerida por escrito, ni la exigencia de la firma, ni la originalidad de la información ni la admisibilidad de fuerza probatoria, por cuanto el Decreto 1747 no contrarió tales disposiciones, sino que se mantuvo acorde con la esencia de las mismas. En efecto, si el suscriptor solo requería usar ciertos mensajes de datos entre él y la entidad emisora, podía acudir a la Entidad de Certificación Cerrada; sin embargo, si necesitaba un respaldo con firma digital, podía solicitar el respectivo certificado ante la Entidad de Certificación Abierta, en ambos casos el mensaje de datos era válido de acuerdo con el uso que se le quisiera dar, es decir, que existe el reconocimiento jurídico invocado. Cuando el suscriptor deseara que la información constara por escrito, podía acudir a cualquiera de las entidades de certificación, para lo cual debía tener en cuenta ante quiénes la quería hacer valer tal como se explicó en precedencia; lo mismo ocurría cuando requiriera usar la firma digital, razón por la cual tampoco se vulneró el artículo 6º de la Ley 527, pues dicho documento escrito gozaba de plena validez para la realización de las transacciones a que hubiere lugar.

COMERCIO ELECTRÓNICO – Principios / PRINCIPIO DE EQUIVALENCIA FUNCIONAL – Alcance

[R]especto de los «principios» aducidos por el actor, según la Ley Modelo de Comercio Electrónico –LMCE- de las Naciones Unidas, la «equivalencia funcional» se basa en «un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico. Por ejemplo, ese documento de papel cumple funciones como las siguientes: proporcionar un documento legible para todos; asegurar la inalterabilidad de un documento a lo largo del tiempo; permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito; permitir la autenticación de los datos consignados suscribiéndolos con una firma; y proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales». Lo anterior significa que la «equivalencia funcional» comprende aplicar al comercio electrónico el principio de la «no discriminación» por tratarse de mensaje de datos, pues pretende que estos produzcan los efectos jurídicos deseados por el emisor tal como si se tratara de

documentos en papel, es decir, sin distinción alguna. En la Guía para la incorporación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico al derecho interno se formularon conceptos jurídicos de no discriminación y neutralidad respecto de los medios técnicos, es decir, que se debe respetar el uso de cualquier tecnología que se utilice o pueda usarse en el futuro a efectos de transmitir un mensaje de datos o firma electrónica, lo que significa que no se pueden favorecer unas tecnologías sobre otras.

MENSAJE DE DATOS – Firma y certificado digital por entidad de certificación abierta / COMERCIO ELECTRÓNICO – Principios / PRINCIPIO DE EQUIVALENCIA FUNCIONAL – No vulneración / ENTIDAD DE CERTIFICACIÓN ABIERTA Autenticidad de la información / SEGURIDAD JURÍDICA en las relaciones informáticas realizadas por vía electrónica - Garantía

[N]o encuentra la Sala que este haya vulnerado los «principios» aducidos por el demandante, por cuanto las disposiciones contenidas en los artículos 4º y 15 numeral 1º del Decreto 1747 (censurados), no afectan la «equivalencia funcional», pues permite que los mensajes de datos por ellas emitidos, sean usados dentro del comercio electrónico para lo cual (como se explicó en precedencia) era necesario tener en cuenta el uso que se les quería dar tal como ocurre en el comercio tradicional, por ejemplo, en los eventos en que ciertas transacciones requieran una firma con presentación personal y otras no; no se afecta el principio de «no discriminación» en la medida en que no prevé mayor valor y eficacia a los documentos de papel; y tampoco afecta lo que el actor denominó como «principio minimalista», por cuanto no exige requisitos adicionales a los estrictamente necesarios para las transacciones que han de efectuarse en el comercio electrónico. En efecto, aunque los certificados emitidos por las Entidades de Certificación Cerrada tenían efectos entre las mismas y el usuario, lo cierto es que el emisor se encontraba en total libertad de acudir a una Entidad de Certificación Abierta, autorizada por la Superintendencia de Industria y Comercio, cuando requiriera que un mensaje de datos fuese respaldado a través de una firma y un certificado digital, tal como ocurre en el comercio tradicional, verbigracia, en los casos en que el interesado necesite una fotocopia autenticada o un documento notariado, se encuentra en libertad de acudir a las entidades respectivas para tales efectos. Se evidencia, entonces, que la norma cuestionada no imponía requisitos adicionales a los citados mensajes de datos, sino que establecía que en caso de que se pretendiera que dichos mensajes fuesen amparados mediante una firma y un certificado digital, solo en ese evento, tal certificado debía ser emitido por una Entidad de Certificación Abierta mas no en el resto de los casos. Lo anterior se encuentra en consonancia con lo exigido en el comercio tradicional, pues cuando en el mismo se requiere de algún documento certificado para la realización de cierta transacción, para su expedición es menester cumplir determinadas exigencias para acreditar tal carácter, pues a través de él se ratifica como cierto el contenido de determinado escrito, por consiguiente, es evidente que en el sub examine no se agregaron requisitos adicionales de los exigidos a un certificado en papel, sino similares, lo que confirma el cumplimiento del principio de la «equivalencia funcional» en el comercio electrónico. […] En efecto, el respaldo del mensaje de datos a través de un certificado y una firma digital, emitido por una Entidad de Certificación Abierta, que en ciertas ocasiones se requería en el comercio electrónico, se encontraba en armonía con los requisitos de forma que en algunos casos se exigen en los documentos de papel en las transacciones efectuadas en el mercado tradicional, en aras de otorgar seguridad jurídica a las mismas.

FUENTE FORMAL: LEY 527 DE 1999 / LEY MODELO DE COMERCIO ELECTRÓNICO LMCE DE LAS NACIONES UNIDAS

NORMA DEMANDADA: DECRETO 1747 DE 2000 (11 de septiembre) GOBIERNO NACIONAL – ARTÍCULO 4 (No anulado) / DECRETO 1747 DE 2000 (11 de septiembre) GOBIERNO NACIONAL – ARTÍCULO 15 NUMERAL 1 (No anulado)

CONSEJO DE ESTADO

SALA DE LO CONTENCIOSO ADMINISTRATIVO

SECCIÓN PRIMERA

Consejera ponente: MARÍA ELIZABETH GARCÍA GONZÁLEZ

Bogotá, D.C., ocho (8) de febrero de dos mil dieciocho (2018)

Radicación número: 11001-03-24-000-2010-00530-00

Actor: MARCO ANTONIO PEREZ USECHE

Demandado: MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO, Y, **MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**

Referencia: Acción de Nulidad

Referencia: Se deniegan las súplicas de la demanda por cuanto los artículos 4º y 15 numeral 1º del Decreto 1747 de 11 de septiembre de 2000, que regulaba lo atinente a los certificados y firmas digitales, no vulneraron la Ley 527 de 18 de agosto de 1999 ni la Ley Modelo de Comercio Electrónico -LMCE- de las Naciones Unidas, aprobada por la Asamblea General de la ONU, en la medida en que no restringieron la autonomía de la voluntad de las partes ni el principio de la «equivalencia funcional», pues si bien es cierto que solo los certificados emitidos por las Entidades de Certificación Cerrada tenían efectos entre la misma y el usuario, también lo es que el interesado se encontraba en total libertad de acudir a una Entidad de Certificación Abierta autorizada por la Superintendencia de Industria y Comercio, cuando requiriera que un mensaje de datos fuese respaldado a través de una firma y un certificado digital. Se evidenció que, por el contrario, los actos acusados, se subsumieron a los principios de la «no discriminación de los mensajes de datos», «minimalista» y el de la «equivalencia funcional».

La Sala decide, en única instancia, la demanda promovida por el abogado **MARCO ANTONIO PEREZ USECHE,** en contra de la **Nación**- **Ministerio de Comercio, Industria y Turismo**, y, **Ministerio de Tecnologías de la Información y las Comunicaciones**, tendiente a obtener la declaratoria de

nulidad de los artículos 4º y 15 numeral 1º del Decreto 1747 de 11 de septiembre de 2000[1], expedido por el Gobierno Nacional.

I.- ANTECEDENTES

I.1.- El actor, en ejercicio de la acción de nulidad consagrada en el artículo 84 del CCA., presentó demanda ante esta Corporación, tendiente a obtener la declaratoria de nulidad de los artículos 4º y 15 numeral 1º del Decreto 1747 de 2000, expedido por el Gobierno Nacional, «*Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales*».

I.2.- El demandante, fundamentó sus hechos en que *«[…] con fecha 11 de septiembre de 2000, el Presidente de la República de Colombia, promulgó el Decreto 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales […]».*

I.3.- En apoyo de sus pretensiones, el actor adujo la violación de los artículos 2º, 5º, 6º, 7º, 8º y 10º de la Ley 527 de 18 de agosto de 1999[2]. En síntesis, señaló los siguientes cargos de violación, así:

Que la Ley Modelo de Comercio Electrónico (1996) de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional –LMCE- sirvió de texto guía principal para la elaboración de la Ley 527 o Ley de Comercio Electrónico[3]. Esta Ley Modelo mediante su texto Guía de la CNUDMI, se basa en dos principios

---

[1] «Por el cual se reglamenta parcialmente la ley 527 de 1999 en lo relacionado con las entidades de certificación, los certificados y las firmas digitales».
[2] «Mediante 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».
[3] A través de la Guía para la Incorporación al Derecho Interno de la Ley Modelo de la CNUDMI

básicos para conocer el valor jurídico de los mensajes de datos: principio de la no discriminación de los mismos y principio de la equivalencia funcional de los mensajes de datos frente a los documentos basados en papel.

Afirmó que, el valor jurídico de los mensajes de datos en Colombia utilizados en las actuaciones entre particulares o actuaciones ante el Estado, conforme al artículo 5º de la Ley 527 que corresponde al artículo 5º de la Ley Modelo de Comercio Electrónico- LMCE-, se basa en el principio de la no discriminación con el propósito de evitar que se restrinja por razones no justificadas, la creación, la gestión, uso y conservación de información generada a través de las denominadas tecnologías de la información.

Explicó que, el mencionado artículo 5º, expresa que no se generarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

Señaló que, en virtud del principio de no discriminación de los mensajes de datos, su valor jurídico debe ser estudiado y analizado conforme a los demás principios de la Ley 527 y a las normas procesales que resulten aplicables.

Precisó que, en desarrollo del principio de la no discriminación, todo servidor público tiene la obligación legal de abordar el estudio científico de validez de los mensajes de datos, que reciba o recaude en desarrollo de su actividad y no puede discriminarlos frente a los documentos basados en papel.

Explicó que, este principio, se reitera en el artículo 10° de la Ley 527 al señalar que en toda actuación administrativa o judicial no se negará la eficacia, validez o

fuerza obligatoria y probatoria de todo tipo de información en forma de un mensaje de datos por el solo hecho de no haber sido presentado en su forma original.

Relató que, a su vez, el artículo 11 de la Ley 527 reafirma el pluricitado principio de la no discriminación de los mensajes de datos frente a los documentos soportados en papel, al señalar que para la valoración de la fuerza probatoria de los mismos, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas.

Sostuvo que, los artículos 6º, 7º y 8º de la Ley 527 establecen el principio equivalente funcional, el cual consiste en determinar «*si las funciones de forma consignadas sobre el papel*», se pueden cumplir con técnicas o métodos asociados con el denominado comercio electrónico.

Alegó que, el artículo 7º de la Ley 527, que es de carácter imperativo, establece los requisitos mínimos que deben ser observados en los mensaje de datos que se utilicen en las actuaciones entre particulares o ante el Estado, acreditándose como un documento firmado.

Manifestó que, dicho artículo 7º, expresa que todo requisito de firma manuscrita que esté establecido en cualquier norma vigente, se podrá observar válidamente con un método de firma electrónica, que cumpla con los siguientes requisitos mínimos o funciones: 1) debe permitir identificar al iniciador de un mensaje de datos (función de identificación); 2) debe servir para indicar que el contenido cuenta con su aprobación (función de autenticación), y, 3) debe ser confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado (función de integridad).

Explicó que, la norma citada permite que los requisitos de firmas que están presentes en el ordenamiento colombiano en normas a nivel nacional, departamental, distrital o municipal, en actuaciones entre particulares o ante el Estado, sean cumplidos con métodos de firma electrónica, siempre y cuando se observen las exigencias expresadas.

Argumentó que, el citado artículo 7º de la Ley 527 establece una categoría jurídica mas no técnica, que al desarrollar el principio de equivalencia funcional persigue que el Estado aplique los requisitos de la Ley 527 caso por caso, sin restringir el uso de nuevas tecnologías o métodos de firma; y para cada categoría de firma, la administración pública debe hacer una adecuación de la misma, frente a los requisitos establecidos en dicho artículo.

Expresó que, los artículos 6º, 7º y 8º de la Ley 527 definen normas imperativas que no pueden ser modificadas de mutuo acuerdo entre las partes, y que se entienden como los requisitos de forma que han de ser considerados como el «*mínimo aceptable*» para determinar la validez de un documento electrónico; sin embargo, la imperatividad de estas normas, no debe entenderse como una invitación a establecer requisitos de forma más estrictos en el derecho interno que los enunciados en la LMCE (principio minimalista).

Aseveró que, el artículo 2º *ibidem*, define la firma digital, la cual integra los elementos técnicos de la misma basada en la tecnología de criptografía de clave pública, es decir, como un valor numérico que se crea con la clave privada del firmante, por lo que para crear firmas digitales se utiliza un programa de computador basado en un procedimiento matemático, denominado algoritmo de creación de firmas.

Arguyó que, la firma digital cambia de un documento a otro en la medida en que los datos de la clave privada se mezclan con los datos de cada documento que sea firmado con la misma clave privada.

Explicó que, para cada documento firmado, se crea una nueva firma digital, pues lo que cambia es la clave privada, por lo que el proceso de verificación de la autenticidad de las firmas se realiza a través de un programa de computador basado en un procedimiento matemático que se denomina algoritmo de verificación de firmas, pues a través de este procedimiento, se comprueba que el documento fue firmado con la clave privada del firmante (autenticidad) y que la información del documento se conserva completa e inalterada (integridad).

Afirmó que, el artículo 28 de la Ley 527 establece expresamente las funciones y atributos jurídicos de la firma digital, el cual resulta aplicable tanto para firmas digitales que se utilicen en relaciones entre particulares, como en relaciones frente al Estado.

Sostuvo que, dicha norma señala que se presume que cuando una firma digital haya sido fijada en un mensaje de datos, el suscriptor del mensaje tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Indicó que, esta presunción es de carácter legal y que admite prueba en contrario, sin embargo, quien pretenda beneficiarse de la misma deberá observar los requisitos del parágrafo del artículo 28 *ibidem*, que prevé expresamente que la firma digital será equivalente si incorpora los siguientes atributos: 1) es única a la persona que la usa; 2) es susceptible de ser verificada; 3) está bajo el control exclusivo de la persona que la usa; 4) está ligada a la información o mensaje, de

tal manera que si éstos son cambiados, la firma digital es invalidada; y, 5) está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

Alegó que, estos atributos de validez, son concurrentes y reiteran los elementos técnicos y de funcionamiento de este tipo de tecnologías.

Argumentó que, el artículo 15 del Decreto 1747 establece requisitos concurrentes para beneficiarse de la presunción de validez del mencionado artículo 28 de la Ley 527, pues en aquél se establecen las denominadas firmas digitales certificadas que son creadas y verificadas con la tecnología de criptografía de clave pública y que, adicionalmente, están respaldadas en certificados digitales por entidades de certificación autorizadas.

Manifestó que, el artículo 4º del Decreto 1747 establece, entre otras, que:

> *«…Los certificados emitidos por las Entidades de Certificación Cerradas deberán indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor. Las entidades deberán informar al suscriptor de manera clara y expresa, previa expedición de los certificados, que éstos no cumplen los requisitos del artículo 15 del presente decreto»*

Señaló que, dicha norma prevé en forma errónea que los certificados digitales emitidos por las Entidades de Certificación Cerradas poseen menor valor que los emitidos por las Entidades de Certificación Abiertas, a pesar de que ellos pueden ofrecer los mismos niveles de confiabilidad técnica y jurídica. La tecnología de emisión de los certificados de creación y verificación de las firmas que usa la Entidad de Certificación Cerrada se basa en algoritmos de «*encripción*» asimétrica, que es la misma tecnología de seguridad que utiliza la Entidad de Certificación Abierta.

Aseveró que, el artículo transcrito, resulta restrictivo del principio de autonomía de la voluntad de las partes para seleccionar el método de firma electrónica que consideren apropiado para los fines de la transacción y le niega efectos jurídicos a un método de firma que es confiable técnica y jurídicamente, por lo que va en contravía de los principios minimalistas de no discriminación y el de equivalencia funcional que sustenta la normativa de la Ley 527.

Explicó que, el citado principio minimalista expresa que todos los estados nacionales que adopten los principios de la LMCE, no deben crear normas que establezcan requisitos adicionales para las firmas electrónicas frente a los requisitos de forma relativos a documentos en papel.

Mencionó que, sobre este último aspecto, el mandato expreso del texto de la Directiva Europea de Firma Electrónica, en su considerando 16, señala que los Estados miembros de la Unión no deben negar efectos jurídicos de las firmas electrónicas utilizadas en sistemas cerrados, aunque también reconoce expresamente el principio de la autonomía de la voluntad de las partes para definir los métodos tecnológicos que se ajusten a sus necesidades particulares y que lo recogen los artículos 14 al 25 de la Ley 527.

Adujo que, la mencionada Directiva Europea señala que ha de respetarse la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas y que, no se debe privar a las que son utilizadas en sistemas cerrados de eficacia jurídica ni de su carácter de prueba en los procesos judiciales.

Arguyó que, el artículo 3º de la Ley 527 señala que en la interpretación de esta ley, habrá de tenerse en cuenta su origen internacional, la necesidad de promover

la uniformidad de su aplicación y la observancia de la buena fe. Además, que las cuestiones relativas a materias que en ella se rijan y que no estén expresamente resueltas serán dirimidas de conformidad con los principios generales en que se inspira.

Afirmó que, el Documento CONPES 3620 de 2009, que define los lineamientos de la Política de Desarrollo e Impulso de Comercio Electrónico en Colombia, señala que los requisitos establecidos en el Decreto 1747 para las Entidades Certificadoras Abiertas de Firmas Digitales, son restrictivos para el desarrollo del comercio electrónico en Colombia y que el Gobierno Nacional debe buscar esquemas alternativos a la firma digital y promover el diseño del mecanismo, para minimizar los requisitos requeridos para autorizar la actividad de las entidades de certificación.

Indicó que, el artículo 2º de la Ley 1341 de 30 de julio de 2009[4], en desarrollo del principio de neutralidad tecnológica, dispone que el Estado garantizará la libre adopción de tecnologías, mediante la promoción de la eficiente prestación de servicios, contenidos en aplicaciones que usen tecnologías de la información y las comunicaciones a través de la garantía de la libre y leal competencia.

Expresó que, ese mismo artículo, en desarrollo del principio de masificación del Gobierno en Línea señala que con el fin de lograr la prestación de servicios eficientes a los ciudadanos, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en el desarrollo de sus funciones.

---

[4] *«Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC-, se crea la Agencia de Espectro y se dictan otras disposiciones».*

Finalmente, manifestó que los artículos 4º y 15 numeral 1º del Decreto 1747 (demandados), resultan restrictivos y violatorios a los principios de neutralidad tecnológica y de masificación del Gobierno en Línea, definidos en la Ley 1341, porque impiden que el sector público utilice certificados emitidos por Entidades de Certificación Cerradas que posean pleno valor jurídico y que las firmas que se vinculen con dichos certificados, gocen de la presunción de no repudio que establece el artículo 28 de la Ley 527.

II-. TRAMITE DE LA ACCIÓN

A la demanda se le imprimió el trámite del procedimiento ordinario, en desarrollo del cual se surtieron las etapas de admisión, fijación en lista, probatoria y alegaciones.

II.1. CONTESTACIONES DE LA DEMANDA

II.1.1. La Nación- Ministerio de Comercio, Industria y Turismo-, a través de apoderada, contestó la demanda, se opuso a la prosperidad de sus pretensiones y fundamentó su oposición, en esencia, en lo siguiente:

Que el Presidente de la República en ejercicio de la atribución constitucional de reglamentar la Ley, prevista en el artículo 189 ordinal 11, mediante el Decreto 1747 reglamentó parcialmente la Ley 527 en lo relacionado con las Entidades de Certificación, los certificados y firmas digitales, es decir, la Parte III de la mencionada Ley, la cual, además, consta de otras dos Partes, Parte I, Parte General; y la Parte II, comercio electrónico en materia de transporte de mercancías.

Afirmó que, el Decreto 1747 en su artículo 1º, con base en las características, requerimientos y actividades de las Entidades de Certificación previstas en los artículos 29 y 30 de la Ley 527, en su artículo 8º, previó dos clases de Entidades de Certificación, la Abierta y la Cerrada, cuya diferencia radica en que los servicios que presta la última de ellas son gratuitos y únicamente comprenden el intercambio de mensajes entre ésta y el suscriptor; en tanto que la Abierta, presta los servicios a título oneroso y su campo de acción se extiende a otros destinatarios, por ende, con diferentes propósitos.

Sostuvo que, si bien las Entidades de Certificación Cerradas operan con mecanismos de infraestructura de clave pública, no ofrecen servicios al público de manera general como sí lo hacen las Entidades de Certificación Abiertas, las cuales basan su operación comercial en la venta de certificados digitales para todo tipo de uso.

Señaló que, esto explica el trato diferente que el citado Decreto 1747 les otorga, pues se vislumbra que los requisitos que debe acreditar la Entidad de Certificación Cerrada ante la Superintendencia de Industria y Comercio, según el artículo 3º del Decreto 1747 no son tan rigurosos como los exigidos a las Entidades de Certificación Abiertas (artículo 5º ibidem).

Argumentó que, del análisis de los artículos 4º y 15 ibidem, y de las diferencias existentes entre las Entidades de Certificación Cerradas y Abiertas frente al artículo 28 de la Ley 527, se evidencia la subjetividad del cargo endilgado por el actor cuando afirma que las disposiciones acusadas otorgan un menor valor jurídico y técnico al certificado expedido por una Entidad de Certificación Cerrada, dado que pasa por alto las características del servicio que presta la referida Entidad, que por estar limitado al intercambio de mensajes entre la Entidad y el

suscriptor, los certificados que expide solo pueden ser usados entre la entidad emisora y el firmante.

Manifestó no estar de acuerdo con el argumento del actor, relativo a que los artículos 4º y 15 numeral 1 del Decreto 1747 violan los principios de neutralidad tecnológica y de masificación del Gobierno en Línea, habida cuenta de que los certificados emitidos por las Entidades de Certificación Cerradas son mensajes de datos[5], los cuales de conformidad con el artículo 10º de la Ley 527 tienen plena validez jurídica y fuerza probatoria.

Explicó que, el artículo 10º *ibidem*, señala que los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones contenidas en el Capítulo VII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

II.1.2. La Nación- Ministerio de Tecnologías de la Información y las Comunicaciones -TIC-, a través de apoderada, contestó la demanda, se opuso a la prosperidad de sus pretensiones y fundamentó su oposición, en esencia, en lo siguiente:

Que le llama la atención que el actor, que participó en la elaboración del texto de la Ley 527, no se percate de que no hay discusión de validez acerca de los Certificados de Entidades Cerradas, sino una limitación en su ámbito, lo cual va perfectamente en línea con la misma en la medida en que permite un uso interno de certificados, que tienen valor general, exactamente como lo tienen los de las Entidades de Certificación Abiertas, tal como lo define su artículo 2º.

---

[5] *«Mensajes de Datos: Información generada, enviada, almacenada o comunicada por medios electrónicos, ópticos o similares, como pueden ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.»*

Indicó que, una cosa es una Entidad Cerrada y otra muy distinta que se varíen las reglas de validez de los mensajes de datos, por lo que considera necesario recordar lo que prevé el artículo 28 ibidem, así:

> *«[…]*
>
> ***ARTÍCULO 28**. Atributos jurídicos de una firma digital. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.*
>
> *[…]».*

Explicó que, dicha Ley declara un valor general respecto de los mensajes de datos, conforme a ciertos requisitos que no son variados por las normas acusadas, por lo que la discusión es más de gusto respecto de lo que hubiera querido la parte demandante, que de fondo.

Expresó que, es cierto que la Ley Modelo UNICTRAL[6] 1996 *«[…] es fundamento de la pluricitada Ley 527 de 1999, pero ni es el único ni se tomó literalmente*», pues la misma contiene importantes innovaciones respecto de la Ley UNCITRAL de 1996, por ser modelo como su nombre lo indica y no «*una suerte de marco obligatorio*».

Arguyó que, el principio de la no discriminación se mantiene, dado que son Certificados con valor pleno, por lo que no vislumbra *«[…]de dónde saca la honorable contraparte que no otorga dicho valor […]*». Lo mismo ocurre con la equivalencia funcional, la cual se mantiene así como con los temas de firma y demás y nada de lo previsto en los artículos demandados afecta lo consagrado en la referida Ley 527.

---

[6] Siglas en inglés que corresponden a United National Commission on International Trade. En español CNUDMI Comisión de las Naciones Unidas para el Derecho Mercantil.

Manifestó que, la extensa y confusa demanda que ha dado lugar a este proceso, se basa en apreciaciones subjetivas poco claras, pues trata de *«[…] hacer parecer diferente el reglamento a lo reglamentado. Lo que se observa una y otra vez es la acusación del presunto "menor valor" en el caso de las entidades certificadoras cerradas […]*»

Precisó que, a su juicio, en cuanto a la no discriminación aducida por el demandante, no se trata de una expresión contenida en la Ley 527, sino de una sugerencia que se hace en la demanda, dado que parece referirse al hecho de que no se discriminará lo electrónico por no estar en papel, sin embargo, ello nada tiene que ver con la discusión, puesto que todo el tema quizá se concentra en la existencia de Entidades Certificadoras Cerradas (cuya existencia no debate la demanda) y el hecho de lo previsto en el numeral 1º del artículo 15 del Decreto 1747.

A su juicio, falla el argumento frente a que los certificados de las Entidades Cerradas tienen menor valor que el de las Entidades Abiertas, puesto que el artículo 4º ibidem lo que preceptúa en realidad es cómo se usan esos certificados.

Aseveró que, no se trata de un caso de menor valor sino de valor distinto, y ello porque el propósito de los certificados emitidos por las Entidades Cerradas no es el mismo que el de las Abiertas, de conformidad con lo establecido en el artículo 1º del Decreto 1747, que define tales entidades, definición de carácter funcional por lo que tal norma no permite comparaciones como las propuestas por el actor, ya que hay supuestos distintos en cada caso.

Afirmó que, el «*principio minimalista*» mencionado por el demandante, tampoco es un concepto de la Ley 527 ni de la Ley Modelo de UNCITRAL de comercio electrónico, sino de otro tipo de normas, en concreto aquellas sobre firma electrónica; sin embargo, dicha Ley tiene una inspiración distinta, es más, se rechaza el hecho de que la demanda trate de inducir a error al Consejo de Estado, puesto que la Firma Europea de Firma Electrónica (Directiva 1999/93/CE), es posterior a la norma en mención.

Sostuvo que, no vale la pena referirse al argumento del Documento CONPES 3620, relativo a los lineamientos para el comercio electrónico ya que el Decreto 1747 de alguna manera es restrictivo al comercio electrónico, por tratarse de «*una afirmación de intención de modificación de dicho decreto, o incluso de la ley.*»

Señaló que, el citado Documento CONPES concluye con la recomendación de la revisión del marco normativo actual, lo cual «*no va ni viene al presente proceso*».

Argumentó que, en cuanto al fondo del debate, la Ley 527 de 1999, no se refiere en realidad a la firma electrónica sino a la firma digital, por lo que advierte que la misma no trató de agotar lo relativo con la firma en mención, «*puesto que el mundo de las discusiones estaba en marcha. De hecho, el término "firma electrónica" no está presente en la Ley 527. No puede entonces llamarse a confusión al respecto. La Ley 527 es una ley general de Intercambio Electrónico de Datos, y solamente en forma parcial de comercio electrónico o de firma digital*».

Manifestó que, una firma electrónica tiene igualmente valor si se trata de un mensaje de datos con las características previstas en la plutricitada Ley 527, es decir, con o sin certificado un mensaje de datos puede tener pleno valor.

Explicó que, lo anterior no quiere decir que si un mensaje no tiene firma digital, entonces no tiene valor como parece sugerir el actor, esto es falso, pues «*nadie ha perdido nada con la existencia de las Entidades Certificadoras Cerradas. Ellas tienen un propósito distinto*», por lo que nada le impide al Gobierno o a cualquiera para acudir a una Entidad Certificadora Abierta, o bien a una extranjera, en los términos del artículo 43 *ibidem*.

II.1.3. La Sociedad ADALID CORP. S.A.S, tercera interesada en las resultas del proceso, a través de apoderado, se pronunció frente a las pretensiones de la demanda. En esencia, efectuó un análisis conceptual de los términos de «*comercio electrónico*», «*mensaje de datos*», «*principio de prevalencia del derecho sustantivo preexistente*», «*principio de neutralidad de redes*», «*principio de la equivalencia funcional*» así como del «*principio de neutralidad tecnológica*» y, precisó:

Que no debe continuar el debate de posibles discriminaciones, producto de la presunción legal de confiablidad y «*apropiabilidad*» asignada en la Ley 527 a los certificados digitales de las Entidades de Certificación Digital.

Aseveró que, para algunos mercados, este certificado puede ser empleado para la salvaguarda del derecho sustantivo de la diligente contemplación de la responsabilidad contractual y extracontractual en las actuaciones estructuradas mediante mensajes de datos y cuyo objeto sea de naturaleza sensible, sujeto a parámetros especiales de responsabilidad jurídica, como ocurre a los comerciantes y a ciertos sectores de la economía, tales como el financiero. Además, aunque no fuere de una naturaleza sensible, este certificado podrá ser empleado por quien lo desee, pero por interpretación sistemática y material, pues no son los únicos modelos de seguridad de la información.

Afirmó que, se podrían emplear otros sistemas de certificación digital, pero desde la prevalencia del derecho sustantivo, dado que lo único que se puede garantizar es que cada rol en la sociedad goce y satisfaga su régimen de derechos, libertades y obligaciones, por lo que todos deben sujetarse a ello, en aras del Estado Social de Derecho.

Sostuvo que, en definitiva es el derecho sustantivo la respuesta a cada caso concreto, mas no un debate de infundadas discriminaciones, máxime cuando en realidad para cada clase de Entidad Certificadora, el Estado lo que promueve es el recto direccionamiento de la economía con niveles y alcances del servicio claramente definidos para cada una, en fomento de la seguridad jurídica.

Señaló que, es imperativo para el Estado cumplir con su deber de lograr economías seguras y amigables para los consumidores, competidores, y en general, para cualquier agente económico, incluso, las mismas entidades públicas, so pena de fallas en el servicio de regulación y reglamentación a su cargo. En ese orden, la regulación que se ha elaborado para el mercado de la certificación digital es un claro desarrollo de la equivalencia funcional en las especialidades de los intervinientes de la sociedad de la información, «*en pro del recto direccionamiento de los mercados de bits, y correspondientes mercados de átomos dependientes de dichos bits.*»

Indicó que, en caso de controversia, se hace necesario que la Entidad demuestre adicionalmente, entre otros, que la firma ha estado bajo el control exclusivo de la persona que la usa de manera permanente, por lo que en el caso de los certificados emitidos por las Entidades de Certificación Cerradas no se pueden utilizar para avalar firmas digitales enviadas a terceros; por tal razón, dichas

entidades no pueden cobrar por su servicio de «*entidad de certificación*» dado que fueron creadas y son utilizadas solo para brindar mayor seguridad a la propia entidad de certificación.

Expresó que, las firmas digitales generadas mediante el uso de certificados digitales emitidos por Entidades de Certificación Abierta, debidamente autorizada por la Superintendencia de Industria y Comercio, cuentan con el mismo valor probatorio y fuerza obligatoria de una firma manuscrita, por lo que los mensajes de datos que estén afectados por una firma digital emitida por estas Entidades de Certificación Abierta, se presumen auténticos.

Arguyó que, los servicios de las entidades de certificación están dirigidos al público en general y no limitan el intercambio de mensajes de datos, puesto que este tipo de Entidades cumple con un estándar de seguridad bastante alto para proteger a los usuarios; le es exigible la adquisición de un seguro con el fin de proteger a los usuarios y terceros que confíen en sus servicios, por si ocurriera un error u omisión del proceso de verificación de la autenticidad.

Manifestó que, la utilización de un certificado digital emitido por una Entidad de Certificación Cerrada autorizada por la Superintendencia de Industria y Comercio, permite de manera única y exclusiva que se realicen comunicaciones electrónicas entre la correspondiente Entidad de Certificación Cerrada y el titular del certificado digital que haya sido emitido por ésta.

Relató que, por lo contrario, los certificados digitales emitidos por Entidades de Certificación Abiertas, también autorizados por la referida Superintendencia, permiten el uso transversal de los certificados, es decir, no restringe el uso del mismo entre el titular del certificado y su entidad emisora, sino que permite que

éste sea utilizado en cualquier ámbito o con cualquier otra entidad o persona diferente de su emisor, lo cual amplía la funcionalidad del certificado, pues el titular podrá efectuar transacciones con cualquier sujeto (persona natural o jurídica) diferente al emisor del certificado digital.

Adujo que, las Entidades de Certificación Cerradas no podrán cobrar dinero ni exigir ninguna contraprestación por la prestación de sus servicios en razón de su utilización única para el intercambio de mensajes entre la Entidad y el titular del certificado digital.

Aseveró que, el uso de las Entidades de Certificación Abiertas, debido al carácter de transversalidad de los certificados que no se limita al intercambio de mensajes entre la entidad y el suscriptor, tal como se explicó en precedencia, permite que estas Entidades de Certificación reciban remuneración por dichos servicios.

Sostuvo que, de acuerdo con el artículo 15 del Decreto 1747 de 2000, los mensajes de datos que estén afectados por una firma digital que se respalde con un certificado expedido por una Entidad Certificación Abierta se presumen auténticos.

Expresó que, las Entidades de Certificación Cerradas se configuran como emisores del mecanismo de seguridad y al mismo tiempo como parte «*confiante*» dentro del proceso de intercambio electrónico de datos, lo cual desvirtúa el objeto principal del «*modelo de Tercero de Confianza*», dado que las Entidades de Certificación Cerradas se establecen como Juez y parte dentro del citado modelo.

Finalmente, precisó que, las Entidades de Certificación Abiertas cumplen con una función completamente diferente, pues éstas juegan un papel exclusivo de

«*Tercero de Confianza*», lo cual fundamenta y sirve de sustento al principio de la tecnología y de la infraestructura de clave pública mundial, que garantiza la existencia de un tercero ajeno a las partes que realizan el intercambio electrónico de datos, asegurando de esta forma que se cumplan todos los presupuestos tanto tecnológicos como legales, que blindan las transacciones electrónicas que sean afectadas con una firma digital emitida por una Entidad de Certificación Abierta, brindándoles todos los atributos y presunciones legales de integridad, posterior consulta y las más importante para este análisis, la presunción de autenticidad inmediata.

II.1.4. La Sociedad de Certificación Digital CERTICAMARA S.A., tercera interesada en las resultas del proceso, a través de apoderado, se pronunció frente a las pretensiones de la demanda. En esencia, adujo lo siguiente:

Que el principio de la no discriminación, contrario a la opinión del actor, no se dirige a impedir una diferenciación entre certificados digitales abiertos y cerrados, sino al hecho de que no podrá un Juez rehusarse a realizar la valoración probatoria de evidencias presentadas en medio electrónico únicamente basándose en tal hecho.

Explicó que, no se podrá negar valor probatorio a un mensaje de datos solo por ser tal, como lo dispone el artículo 10° de la Ley 527, el cual permite al Juez aplicar las reglas de la sana crítica a que se refieren las normas de derecho procesal para realizar la valoración probatoria, pues dicha norma reconoce que se podrá negar la eficacia, validez o fuerza probatoria u obligatoria a los mensajes de datos por otros factores diferentes a la forma en que dichos mensajes fueron presentados.

Afirmó que, el concepto de «*mínimo aceptable*» a que se refiere la Guía de Incorporación de la Ley Modelo de Comercio Electrónico se predica únicamente en el sentido de que las normas contenidas en el Capítulo II han de ser imperativas, por ende, deberá reconocerse a los mensajes de datos el equivalente funcional de los escritos, firma y original, de tal manera que las legislaciones internas no establezcan más requisitos para la equivalencia funcional en los mensajes de datos ni se nieguen efectos jurídicos a tales mensajes de datos solo por su naturaleza electrónica.

Sostuvo que, la Ley Modelo, por su carácter de «*ley*», no tiene por objeto ni debe *«[…] regular todos los pormenores del empleo del comercio electrónico […]*» al interior de los países, pues existen numerosas circunstancias que hacen que la implementación de un instrumento de armonización legal como este sea diferente en cada País donde se adopte, y en virtud de esta diferencia, la CNUDMI[7] reconoce que «*el Estado promulgante tal vez desee dictar un reglamento para pormenorizar los procedimientos de cada uno de los métodos autorizados por la Ley Modelo a la luz de las circunstancias peculiares y posiblemente variable de ese Estado*».

Señaló que, la Guía de Incorporación de la Ley Modelo de Firmas Electrónicas de 2001 señala claramente que los requisitos que impongan los Gobiernos Nacionales en materia de firma electrónica «*podrían, por ejemplo, prescribir el uso de una técnica de firma especialmente concebida en ciertas situaciones especificadas o podrían fijar una pauta superior o inferior a la establecida en el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (y en el artículo 6 de la Ley Modelo)*».

---

[7] *Comisión de las Naciones Unidas para el Derecho Mercantil.*

Argumentó que, los requisitos establecidos en el numeral 11 del artículo 189 de la Carta Política, se cumplen a cabalidad en la referida Ley 527, ya que por una parte, esta determina de manera general los requisitos para la construcción de las Entidades de Certificación, lo que conduce a la necesidad de reglamentar; y, por la otra, no existe ninguna disposición constitucional o de otra jerarquía que establezca que los temas asociados con las Entidades de Certificación y las firmas digitales solamente pueden ser objeto de regulación legal. Además, en su artículo 28, numeral 5º, establece que es el Gobierno el que determinará los requisitos adicionales frente a la atribución jurídica de la firma digital.

Indicó que, en virtud de lo anterior, no existe ningún impedimento para que el Gobierno ejerza su potestad reglamentaria sobre aquellos aspectos relacionados con las Entidades de Certificación, las firmas digitales y lo que estime conveniente.

Expresó no entender el decir del actor, relativo a que los artículos 4º y 5º del Decreto 1747 violan el principio de la autonomía privada por reglamentar expresamente materias que el legislador excluyó de la regulación privada, es decir, el artículo 28 de la Ley 527, por cuanto al analizar la materia que se regula, resulta clara la razón de esta exclusión, la confiabilidad de los métodos de firma (especialmente en la firma digital certificada por una entidad abierta) no sólo está involucrado el interés de las partes de una transacción, sino la de terceros que con seguridad tendrán acceso a esa información, les será oponible el documento firmado, y confiarán en su fuerza probatoria.

Arguyó que, la Superintendencia de Industria y Comercio es la encargada de dar la respectiva autorización para que las Entidades de Certificación Abiertas puedan dar certificados cumpliendo con el requisito mencionado en la sentencia C-831 de 2001, por medio de la cual la Corte Constitucional reconoció que dichas Entidades

son las encargadas de facilitar y garantizar las transacciones comerciales, por medios electrónicos o diferentes a los estipulados en papel, por lo que ostentan un grado alto de confiabilidad y por ende, se hacen merecedoras de un control ejercido por un ente público el cual redunda en beneficio de la seguridad jurídica del comercio electrónico.

Manifestó que, la Superintendencia de Industria y Comercio es la encargada de dar la autorización para que las Entidades de Certificación Abierta puedan expedir constancias que cumplan con los requisitos mencionados en la sentencia C-831 de 8 de agosto de 2001[8], es decir, de carácter público.

Relató que, el Decreto 1747 determina unos requisitos especiales y detallados para las Entidades de Certificación Abierta con el fin de garantizar que el servicio público prestado por estas Entidades no defraude a sus usuarios en general; con estos requisitos, se pretende que tales entidades cumplan los más altos estándares de confiabilidad, para de esta forma materializar la finalidad social del Estado.

Alegó que, por su parte, las Entidades de Certificación Cerrada no cumplen con requisitos para prestar un servicio público, razón por la cual mal podría la reglamentación acceder a un sistema que no cumple con los estándares mínimos, ni que se le permita a un tercero confiar en los certificados digitales emitidos por aquellas ni que tenga los mismos efectos jurídicos de un sistema que sí los tiene.

Aseveró que, el hecho de que se le otorgue una presunción a la firma digital certificada por una Entidad de Certificación Abierta, no significa que la misma sea irrefutable.

---

[8] *Magistrado Ponente doctor ALVARO TAFUR GALVIS*

Adujo que, la presunción legal a que hace referencia el artículo 28 de la Ley 527 no consiste en un juicio anticipado con el cual se desconozca el valor probatorio de otros tipos de firmas, pues la presunción de dicho artículo corresponde a un «*[…] típico procedimiento de técnica jurídica adoptado por el legislador, en ejercicio de su facultad de configuración de las instituciones procesales, con el fin de convertir en derecho lo que simplemente es una suposición fundada en hechos o circunstancias que generalmente ocurren, ante el riesgo de que la dificultad de la prueba pueda significar la pérdida de ese derecho afectando bienes jurídicos de importancia para la sociedad […]*».

Expresó que, el mayor nivel de exigencia que se impone a las Entidades de Certificación Abierta, justifica la diferencia en sus efectos jurídicos.

Explicó que, los artículos 826 y 827 del Código de Comercio consagran los dos únicos tipos de firma existentes en la legislación comercial. El primero, establece como regla general la necesidad de que las firmas sean autógrafas, es decir, manuscritas por su autor; el segundo, restringe el uso de las firmas mecánicas a «*los negocios en que la ley o la costumbre lo admitan*».

Argumentó que, el artículo 7º de la Ley 527 señala que «*[…] Cuando cualquier norma exija la presencia de una forma o establezca ciertas consecuencias de 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 […]*».

Manifestó que, de lo anterior se tiene que en desarrollo del principio de neutralidad tecnológica para firmar electrónicamente un documento, la Jurisprudencia ha acuñado el término firma electrónica para cualquier firma que cumpla con los requisitos arriba mencionados; sin embargo, para que exista dicha firma electrónica, el método utilizado debe ser «*[…] tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado […]*», por lo que no cualquier método se puede usar para firmar electrónicamente un documento; le corresponderá al Juez, siguiendo las reglas de la sana crítica, establecer cuándo un método particular cumple con los requisitos del literal b) y permite, por tanto, la aplicación del equivalente funcional.

Indicó que, dada la eventual dificultad de probar la confiabilidad de los métodos de firma, la Ley 527 estableció una presunción en favor de un tipo especial de firma, a saber, la firma digital, definida en el artículo 2º ibidem, en una especie de «*segundo nivel*» de una escalada probatoria, tal como lo consagra el artículo 28, que prevé que: «*[…] cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo […]*»

Señaló que, la intención del legislador es clara, dado que una firma manuscrita corresponde a la regla general en materia comercial y por tanto, es el tipo de firma más sensible jurídicamente, por lo que corresponde al Ejecutivo la reglamentación de los requisitos que deben configurarse para garantizar este efecto jurídico.

Precisó que, en vista de la diferencia entre los requisitos a cumplir por las Entidades de Certificación Abiertas y Cerradas, el «*reglamentador*» reconoció la importancia de que este segundo tipo de entidades informara a sus suscriptores

que sus certificados no cumplen con los requisitos y efectos definidos para las firmas digitales acreditadas por Entidades de Certificación Abierta.

Arguyó que, la diferencia en los requisitos de constitución y la regulación de funcionamiento es la que justifica los diferentes efectos que tienen los correspondientes certificados digitales, pues mal podría un certificado de una Entidad de Certificación Cerrada tener los mismos efectos cuando estas entidades actúan como Juez y parte dentro de una transacción.

Indicó que, como los certificados de estas entidades tan solo se pueden usar para la comunicación con la misma entidad, es ineludible que sea una de las partes de una comunicación electrónica de estas entidades la que provea las garantías de autenticidad e integridad.

Explicó que, sin embargo, esta entidad además de tener estas funciones, tiene un interés propio en la transacción subyacente cuya seguridad está garantizando, pues, es obvio que esto genera un conflicto de intereses, dado que la entidad tiene que actuar de forma imparcial para proteger la autenticidad e integridad de la comunicación, al mismo tiempo que tiene que actuar también de acuerdo con su interés propio en la transacción.

Alegó que, las Entidades de Certificación Abierta no tienen este conflicto de intereses, son terceros de confianza, ajenos a las transacciones que se usan en sus certificados, no tienen ningún interés de favorecer a ninguna de las partes.

Afirmó que, la existencia de este conflicto de intereses en las Entidades de Certificación Cerrada incrementa los riesgos de corrupción del sistema.

III-. ALEGATO DEL MINISTERIO PÚBLICO

El señor Agente del Ministerio Público, considera que deben desestimarse los cargos formulados por el demandante, por lo siguiente:

Que el artículo 28 de la Ley 527 establece atributos de la firma digital, cuyo resultado es tener la misma fuerza y efectos que el uso de una firma manuscrita; tales atributos son: 1) Es única a la persona que la usa; 2) Es susceptible de ser verificada; 3) Está bajo el control exclusivo de la persona que la usa; 4) Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalida; y 5) Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

Señaló que, en el ámbito estrictamente jurídico, existe una norma que fija unos atributos, la Ley 527, con los cuales una firma digital pude tener la misma fuerza y efectos de la manuscrita, lo que se ha denominado equivalencia funcional (para el caso de la firma, se encuentra establecida en el artículo 7º *ibidem*).

Explicó que, uno de esos atributos le permiten al Gobierno Nacional, efectuar la reglamentación que señala claramente que cuando un mensaje de datos se firme digitalmente y esa firma sea respaldada por un certificado digital, este mensaje de datos cumplirá los tributos señalados en el artículo 28 de la referida Ley 527 y, en efecto, la firma manuscrita tendrá los mismos efectos de la digital, a condición de que el certificado sea emitido por una entidad de certificación abierta autorizada por la Superintendencia de Industria y Comercio.

Argumentó que, el artículo 15 *ibidem* se encuentra conforme al ordenamiento jurídico, pues para que la firma digital sea equiparable a la manuscrita, el certificado que la respalda debe provenir de una Entidad de Certificación Abierta.

Alegó que de acuerdo con la pluricitada Ley 527, el Gobierno Nacional adoptó la respectiva reglamentación del principio de masificación del Gobierno en Línea mediante el Decreto 1151 de 14 de abril de 2008[9], el cual estableció una serie de fases para la implementación del citado Gobierno en Línea (artículo 5°) y un cronograma para su implementación.

Afirmó que, el actor olvidó la consulta de este Decreto Reglamentario que da cuenta de la implementación del programa de Gobierno en Línea, por lo que no se evidencia la restricción del principio de masificación.

Adujo que, frente al principio de neutralidad tecnológica el argumento debe descartarse, toda vez que las normas no están proponiendo la adopción de una tecnología específica para las firmas digitales, simplemente señalan que estas se pueden favorecer de la presunción del artículo 25 de la Ley 527, siempre que estén respaldadas por una Entidad de Certificación Abierta.

IV-. CONSIDERACIONES DE LA SALA

En el presente asunto, el señor **MARCO ANTONIO PEREZ USECHE** solicitó la nulidad de los artículos 4º[10] y 15 numeral 1º[11] del Decreto 1747, expedido por el Gobierno Nacional, «***Por el cual se reglamenta parcialmente la Ley 527 de***

---

[9] «Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la ley 962 de 2005, se dictan otras disposiciones».

[10]«[…]
***ARTÍCULO 4º.** Información en certificados. Los certificados emitidos por las entidades de certificación cerradas deberán indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor. Las entidades deberán informar al suscriptor de manera clara y expresa, previa expedición de los certificados, que éstos no cumplen los requisitos del artículo 15 del presente decreto.*
[…]».

[11] «[…]
***ARTÍCULO 15.** Uso del certificado digital. Cuando quiera que 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 el parágrafo del artículo 28 de la Ley 527 de 1999, sí:*
1. El certificado fue emitido por una entidad de certificación abierta autorizada para ello por la Superintendencia de Industria y Comercio.
[…]»

1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales».

Se advierte que mediante memorial visible a folio 223 del expediente, el actor puso de presente que el Decreto 333 de 19 de febrero de 2014, expedido por el Gobierno Nacional, *«Por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012*[12]*»* derogó el Decreto 1747, en censura.

Al respecto, la Sala precisa que, no obstante la derogatoria de la norma acusada, es menester entrar a estudiar su legalidad habida cuenta de que, por un lado, ésta causó efectos jurídicos y por el otro, continúa amparada por la presunción de legalidad que la protege, pues tal y como lo ha sostenido esta Corporación en reiterada jurisprudencia[13], solamente la declaratoria de nulidad puede hacer desaparecer del mundo jurídico un acto administrativo, no así su pérdida de vigencia, derogatoria o revocatoria; en consecuencia, el Juez siempre está obligado a analizarlo de fondo, en virtud de los efectos que se hubieran podido producir mientras el acto conservó su vigencia.

Se vislumbra que los artículos 4º y 15 numeral 1º del Decreto 1747 (acusados) establecían, respectivamente, que los certificados emitidos por las Entidades de Certificación Cerradas debían indicar expresamente que sólo podrían ser usados entre la entidad emisora y el suscriptor, por lo que los mismos no producirían los efectos de una firma digital como tal; y, que si el certificado era emitido por una Entidad de Certificación Abierta autorizada por la Superintendencia de Industria y Comercio, se tendrían por satisfechos los atributos exigidos para una firma digital

---

[12] «*Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.»*

[13] *Sala Plena de lo Contencioso Administrativo, sentencia de 14 de enero de 1991 expediente S - 157, Consejero Ponente doctor Carlos Gustavo Arrieta Padilla.* Zara
te.

cuando el suscriptor firmase digitalmente un mensaje de datos con su clave privada, y fuese respaldada mediante un certificado digital.

A juicio del demandante, el hecho de que los artículos cuestionados le otorgaran menor valor a los certificados digitales expedidos por las Entidades de Certificación Cerrada frente a los emitidos por las Entidades de Certificación Abierta, resultaba restrictivo del principio de autonomía de la voluntad de las partes para seleccionar el método de firma electrónica que consideraran apropiado para los fines de la transacción y le negaba efectos jurídicos a un método de firma que resultaba confiable técnica y jurídicamente, por lo que, consideró, que las disposiciones demandadas se encuentran en contravía del «*principio minimalista*» que sustenta la Ley 527 expedida con fundamento en la Ley Modelo de Comercio Electrónico –LMCE- de las Naciones Unidas, para lo cual se emitió la Guía para su Incorporación al Derecho Interno de la Ley Modelo de la CNUDMI.

Igualmente, estimó que se vulneró el principio de la «*no discriminación de los mensajes de datos»* y el de la «*equivalencia funcional»* de los mismos, frente a los documentos basados en papel, por crearse requisitos adicionales para las firmas electrónicas que los exigidos en los documentos tradicionales.

La Sala procede, entonces, a determinar si conforme a las anteriores argumentaciones, el Gobierno Nacional al expedir los artículos 4º y 15 numeral 1º del Decreto 1747, vulneró los siguientes artículos de la Ley 527[14], que prevén:

> «***ARTICULO 2o. Definiciones****. Para los efectos de la presente ley se entenderá por:*

---

[14] Y por ende, la Ley Modelo de Comercio Electrónico –LMCE- de las Naciones Unidas, aprobada por la Asamblea General de la ONU, mediante Resolución 51/162 de 1996, que sirvió de texto guía para la expedición de la Ley 527.

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

(…)

c) Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

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;

[…]»

*«**ARTÍCULO 5º. Reconocimiento jurídico de los mensajes de datos**. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.»*

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

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

*«**ARTÍCULO 7º. Firma.** [Reglamentado por el Decreto Nacional 2364 de 2012.] 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.»

> ***«ARTÍCULO 8º. Original****. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:*
>
> *a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;*
>
> *b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.*
>
> *Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.»*
>
> ***«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.»*

Al analizar la normativa anterior junto con los artículos demandados, no encuentra la Sala que estos hayan vulnerado aquella como tampoco la Ley Modelo de Comercio Electrónico –LMCE- de las Naciones Unidas, aprobada por la Asamblea General de la ONU[15], pues el hecho de que el acto acusado hubiese establecido determinados parámetros para que cada entidad de certificación ejerciera su función, no significa que se hubiera alterado la esencia prevista para estas en el literal d) del artículo 2º de la Ley 527.

La norma al referirse a la entidad de certificación, en general, señala que es la persona «*autorizada conforme a la presente ley*», que emite, entre otras, certificados en relación con firmas digitales, es decir, que dicha función la realiza de acuerdo con las facultades y directrices establecidas por la Ley 527.

---

[15] *Fundamento de la Ley 527*

El artículo 30 *ibidem*, respecto de las funciones de dichas entidades, prevé:

> ***«ARTÍCULO 30.*** *Actividades de las entidades de certificación. [Modificado por el art. 161, Decreto Nacional 019 de 2012]. Las entidades de certificación* ***autorizadas por la Superintendencia de Industria y Comercio*** *para prestar sus servicios en el país,* ***podrán*** *realizar, entre otras, las siguientes actividades:*
>
> *1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.*
>
> *2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.*
>
> *3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la presente ley.*
>
> *4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.*
>
> *5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.*
>
> *6. Ofrecer los servicios de archivo y conservación de mensajes de datos.»*

Conforme a lo anterior, es claro que la norma transcrita indica que las entidades de certificación pueden realizar cualquiera de las funciones allí mencionadas, entre otras.

En efecto, el acto demandado indicó que las Entidades de Certificación Abierta emitirían certificados que tendrían por satisfechos los atributos exigidos para una firma digital, en cambio, los transmitidos por las Entidades de Certificación Cerradas sólo podrían ser usados entre la entidad emisora y el suscriptor sin producir efectos de una firma digital, lo cual se encuentra acorde tanto con la norma transcrita como con el el literal d) del artículo 2º del mismo estatuto, pues dichas entidades continuaron ofreciendo y/o facilitando servicios de registro y estampado cronológico de la transmisión y recepción de datos, entre otras, por lo

que según la actividad comercial a desarrollar, en el caso de requerirse una firma digital, el interesado podía acudir a la Entidad de Certificación Abierta, la cual fue la que el acto acusado autorizó para tales efectos, conforme a los requisitos que la misma Ley 527 previó para las referidas firmas (artículo 28). Aspecto del que se hará referencia más adelante.

Tampoco se vislumbró que los artículos 4º y 15 numeral 1º del Decreto 1747 hayan violado el concepto otorgado por la Ley 527 a los mensaje de datos, pues no se establece que las plurimencionadas entidades de certificación al transmitirlos afectaran las características descritas para estos en el literal a) del artículo 2º *ibidem*, habida cuenta que al ser difundidos conservaban su naturaleza, de constituirse en la *«información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares*».

En cuanto a la alegada vulneración del literal c) del artículo 2º de la Ley 527, que define a la firma digital, la Sala no observa tal violación, pues, por un lado, la Entidad de Certificación Abierta al transmitir la referida firma digital debía cumplir las exigencias establecidas para tenerla como tal, ya que estaba obligada a someterse a las directrices previstas en el artículo 28 de la Ley 527 que determinó sus atributos[16]; y por el otro, comoquiera que los datos difundidos por la Entidad de Certificación Cerrada no se constituían en una firma digital, al disponer la norma acusada que dichas entidades debían indicar expresamente que los mensajes por estas transmitidos no producirían los efectos de la citada firma, se

---

[16] *«**ARTÍCULO 28**. Atributos jurídicos de una firma digital. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.*
***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 éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.»

salvaguardó la norma que la definió, toda vez que para ser emitida, la entidad debía estar autorizada y además, debía atenerse a las propiedades exigidas por la Ley en mención.

De igual forma, no se encontró que las normas censuradas vulneraran el reconocimiento jurídico de los mensajes de datos[17], ni la información requerida por escrito[18], ni la exigencia de la firma[19], ni la originalidad de la información[20] ni la admisibilidad de fuerza probatoria[21], por cuanto el Decreto 1747 no contrarió tales disposiciones, sino que se mantuvo acorde con la esencia de las mismas.

En efecto, si el suscriptor solo requería usar ciertos mensajes de datos entre él y la entidad emisora, podía acudir a la Entidad de Certificación Cerrada; sin embargo, si necesitaba un respaldo con firma digital, podía solicitar el respectivo certificado ante la Entidad de Certificación Abierta, en ambos casos el mensaje de datos era válido de acuerdo con el uso que se le quisiera dar, es decir, que existe el reconocimiento jurídico invocado.

Cuando el suscriptor deseara que la información constara por escrito, podía acudir a cualquiera de las entidades de certificación, para lo cual debía tener en cuenta ante quiénes la quería hacer valer tal como se explicó en precedencia; lo mismo ocurría cuando requiriera usar la firma digital, razón por la cual tampoco se vulneró el artículo 6º de la Ley 527, pues dicho documento escrito gozaba de plena validez para la realización de las transacciones a que hubiere lugar.

En cuanto a la originalidad y la admisibilidad y fuerza probatoria de los mensajes

---

[17] *Artículo 5º de la Ley 527*
[18] *Artículo 6º de la Ley 527*
[19] *Artículo 7º de la Ley 527*
[20] *Artículo 8º de la Ley 527*
[21] *Artículo 10º de la Ley 527*

de datos, no encuentra la Sala cómo la emisión de los mismos por parte de las entidades de certificación pudiese llegar a alterar tales características en los mensajes de datos, por el contrario, al regularse los certificados que estas emitían se aseguraba la eficacia de los mismos, en ningún momento las disposiciones censuradas le restan originalidad ni admisibilidad como medios de prueba a las certificaciones emitidas por las pluricitadas entidades, por el contrario, al emitir los referidos certificados les otorga fuerza legal.

Ahora bien, respecto de los «*principios*» aducidos por el actor, según la Ley Modelo de Comercio Electrónico –LMCE- de las Naciones Unidas, la «*equivalencia funcional*» se basa en «*un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico. Por ejemplo, ese documento de papel cumple funciones como las siguientes: proporcionar un documento legible para todos; asegurar la inalterabilidad de un documento a lo largo del tiempo; permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito; permitir la autenticación de los datos consignados suscribiéndolos con una firma; y proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales*».

Lo anterior significa que la «*equivalencia funcional*» comprende aplicar al comercio electrónico el principio de la «*no discriminación*» por tratarse de mensaje de datos, pues pretende que estos produzcan los efectos jurídicos deseados por el emisor tal como si se tratara de documentos en papel, es decir, sin distinción alguna.

En la Guía para la incorporación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico al derecho interno se formularon conceptos jurídicos de no

discriminación y neutralidad respecto de los medios técnicos, es decir, que se debe respetar el uso de cualquier tecnología que se utilice o pueda usarse en el futuro a efectos de transmitir un mensaje de datos o firma electrónica, lo que significa que no se pueden favorecer unas tecnologías sobre otras.

Considera el actor que el acto acusado afecta también el «*principio minimalista*», el cual si bien no se menciona en forma expresa en la LMCE, se entiende implícito en la misma, pues dicha preceptiva al precisar el criterio del «*equivalente funcional*» indica que este no debe dar lugar a que se impongan normas de seguridad más estrictas a los usuarios del comercio electrónico (con el consiguiente costo) que las aplicables a la documentación consignada sobre papel, es decir que su validez no debe implicar cargas adicionales, sino, por el contrario, mínimas.

Así mismo, la Ley Modelo de Comercio Electrónico –LMCE- de las Naciones Unidas indica que la documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, con mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos, con tal que se observen ciertos requisitos técnicos y jurídicos.

Examinado lo anterior junto con el acto cuestionado, no encuentra la Sala que este haya vulnerado los «*principios*» aducidos por el demandante, por cuanto las disposiciones contenidas en los artículos 4º y 15 numeral 1º del Decreto 1747 (censurados), no afectan la «*equivalencia funcional*», pues permite que los mensajes de datos por ellas emitidos, sean usados dentro del comercio electrónico para lo cual (como se explicó en precedencia) era necesario tener en cuenta el uso que se les quería dar tal como ocurre en el comercio tradicional, por

ejemplo, en los eventos en que ciertas transacciones requieran una firma con presentación personal y otras no; no se afecta el principio de «*no discriminación*» en la medida en que no prevé mayor valor y eficacia a los documentos de papel; y tampoco afecta lo que el actor denominó como «*principio minimalista*», por cuanto no exige requisitos adicionales a los estrictamente necesarios para las transacciones que han de efectuarse en el comercio electrónico.

En efecto, aunque los certificados emitidos por las Entidades de Certificación Cerrada tenían efectos entre las mismas y el usuario, lo cierto es que el emisor se encontraba en total libertad de acudir a una Entidad de Certificación Abierta, autorizada por la Superintendencia de Industria y Comercio, cuando requiriera que un mensaje de datos fuese respaldado a través de una firma y un certificado digital, tal como ocurre en el comercio tradicional, verbigracia, en los casos en que el interesado necesite una fotocopia autenticada o un documento notariado, se encuentra en libertad de acudir a las entidades respectivas para tales efectos.

Se evidencia, entonces, que la norma cuestionada no imponía requisitos adicionales a los citados mensajes de datos, sino que establecía que en caso de que se pretendiera que dichos mensajes fuesen amparados mediante una firma y un certificado digital, solo en ese evento, tal certificado debía ser emitido por una Entidad de Certificación Abierta mas no en el resto de los casos.

Lo anterior se encuentra en consonancia con lo exigido en el comercio tradicional, pues cuando en el mismo se requiere de algún documento certificado para la realización de cierta transacción, para su expedición es menester cumplir determinadas exigencias para acreditar tal carácter, pues a través de él se ratifica como cierto el contenido de determinado escrito, por consiguiente, es evidente que en el *sub examine* no se agregaron requisitos adicionales de los exigidos a un

certificado en papel, sino similares, lo que confirma el cumplimiento del principio de la «*equivalencia funcional*» en el comercio electrónico.

Al respecto, la Guía para la Incorporación al Derecho Interno de la Ley Modelo de la CNUDMI, precisó, lo siguiente:

> *«17. Un mensaje de datos no es, de por sí, el equivalente de un documento de papel, ya que es de naturaleza distinta y no cumple necesariamente todas las funciones imaginables de un documento de papel.* ***Por ello se adoptó en la Ley Modelo un criterio flexible que tuviera en cuenta la graduación actual de los requisitos aplicables a la documentación consignada sobre papel****: al adoptar el criterio del "equivalente funcional",* ***se prestó atención a esa jerarquía actual de los requisitos de forma, que sirven para dotar a los documentos de papel del grado de fiabilidad, inalterabilidad y rastreabilidad que mejor convenga a la función que les haya sido atribuida****…»*

En efecto, el respaldo del mensaje de datos a través de un certificado y una firma digital, emitido por una Entidad de Certificación Abierta, que en ciertas ocasiones se requería en el comercio electrónico, se encontraba en armonía con los requisitos de forma que en algunos casos se exigen en los documentos de papel en las transacciones efectuadas en el mercado tradicional, en aras de otorgar seguridad jurídica a las mismas.

Frente a este punto, la Corte Constitucional en sentencia C-662 de 8 de junio de 2000, Magistrado Ponente doctor FABIO MORÓN DÍAZ[22], señaló:

> *«[…]*
>
> *3.3. Entidades de certificación.*
>
> *Uno de los aspectos importantes de este proyecto, es la posibilidad de que un ente público o privado con poderes de certificar,* ***proporcione la seguridad jurídica a las relaciones comerciales por vía informática****. Estos entes son las entidades de certificación, que* ***una vez autorizadas****, están facultados para: emitir certificados en relación con claves criptográficas de todas las personas, ofrecer o*

[22] *Por la que se declararon 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 1999.*

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****.*

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****.*

[…]» (Subrayas y negrillas fuera del texto)

Así, pues, el hecho de que se hubiese asignado la atribución de una firma digital y el carácter certificado a un mensaje de datos expedido por las Entidades de Certificación Abierta, no presuponía ningún espíritu restrictivo sino de **seguridad jurídica** a las relaciones informáticas realizadas por vía electrónica, equivalente, como ya se dijo, al comercio tradicional.

En este orden de ideas, es evidente que el acto acusado no contradecía la Ley 527 ni lo dispuesto en la Guía para la Incorporación al Derecho Interno de la Ley Modelo de la CNUDMI[23] sobre comercio electrónico, pues, como ya se dijo, los artículos 4º y 15, numeral 1, del Decreto 1747 se subsumieron en los criterios de la «*no discriminación de los mensajes de datos»,* «*minimalista*» y el de la «*equivalencia funcional»*, habida cuenta de que no se restringió el uso de la firma digital, que era otorgada la Entidad de Certificación Abierta a la que podía acudir el emisor sin límite alguno; los requisitos exigidos para tener una firma digital como tal, fueron mínimos y los mensajes de datos que se fuesen a utilizar sin necesidad de ser elevados al rango de firma digital surtía efectos entre la entidad emisora y el suscriptor. Se mantuvo la equivalencia funcional, en la medida que dependiendo de la transacción comercial, tal como ocurre en el comercio tradicional, ciertos mensajes de datos podrían ser emitidos por las Entidades de Certificación

---

[23] Publicada por las Naciones Unidas, Nueva York, 1999

Abiertas, en aras de elevar su rango de firma digital con el objeto de otorgarles seguridad jurídica.

Consecuente con lo anterior, la Sala denegará las súplicas de la demanda, como en efecto se dispondrá en la parte resolutiva de esta providencia.

En mérito de lo expuesto, el Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Primera, administrando justicia en nombre de la República y por autoridad de la Ley,

F A L L A :

PRIMERO.- DENIÉGANSE las súplicas de la demanda, de conformidad con las razones expuestas en la parte motiva de esta providencia.

SEGUNDO.- DEVUÉLVASE al actor la suma de dinero depositada para gastos ordinarios del proceso que no fue utilizada.

TERCERO.- Tiénese como apoderada del Ministerio de Tecnologías de la Información y las Comunicaciones a la doctora **SONIA NAYIBE SÁNCHEZ BOTELLO**, de conformidad con el poder y los documentos anexos visibles a folios 266 a 274 del expediente.

CÓPIESE, NOTIFÍQUESE Y CÚMPLASE.

Se deja constancia de que la anterior sentencia fue leída, discutida y aprobada por la Sala en la sesión del día 8 de febrero de 2018.

HERNANDO SÁNCHEZ SÁNCHEZ **MARÍA ELIZABETH GARCÍA GONZÁLEZ**

Presidente

OSWALDO GIRALDO LÓPEZ