

Los mensajes de datos y las firmas electrónicas en los tribunales venezolanos

Data messages and electronic signatures in the Venezuelan courts

Nayibe Chacón Gómez*

José Zapata Figueroa**

Recibido el 10/08/2017 - Aprobado el 09/10/2017

* Doctora en Ciencias, Mención Derecho; Especialista en Derecho Mercantil; Investigadora-Docente adscrita al Instituto de Derecho Privado y Jefa de la Cátedra de Derecho Mercantil de la Escuela de Derecho de la Facultad de Ciencias Jurídicas y Políticas de la Universidad Central de Venezuela.
nayibe.chacon@gmail.com

** Abogado. Cursante de la Especialización en Derecho Mercantil del Centro de Estudios de Postgrado de la Facultad de Ciencias Jurídicas y Políticas de la Universidad Central de Venezuela.
zapata74jesus@gmail.com

Resumen

En Venezuela la adecuación tecnológica ha tenido lugar desde la entrada en vigencia de la Constitución de 1999 y se consolida con la publicación del Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas del año 2000, cuyo origen y contenido son examinados en la primera parte de esta investigación. A través de la elaboración de un cuadro descriptivo en la segunda parte de este artículo se analiza cómo ha sido el tratamiento por parte de los tribunales patrios a dichas figuras, dando mayor atención a las decisiones que han versado sobre el reconocimiento y valor probatorio de los mensajes de datos y firmas electrónicas.

Palabras clave: Mensajes de datos, firma electrónica, documento electrónico.

Abstract

In Venezuela, technological adaptation has taken place since the entry into force of the 1999 Constitution, and had its point of no return with the publication of the Decree-Law on Data Messages and Electronic Signatures, whose origin and content are examined in the first part of this research. Through the elaboration of a descriptive table, the second part of this article analyses how the national courts have dealt with these figures, giving greater attention to decisions on the recognition and evidentiary value of data messages and electronic signatures.

Keywords: Data Messages, Electronic Signature, Electronic Document.

Los mensajes de datos y las firmas electrónicas en los tribunales venezolanos

Presentación

En Venezuela la incorporación de las tecnologías de información y comunicación, han revestido no solamente un carácter de hecho social sino también se han agregado al catálogo de derechos de los ciudadanos consagrados en la Constitución del año 1999, donde se establece el empleo de las tecnologías como herramientas para el desarrollo del país.

En este sentido, el marco jurídico venezolano se ha acondicionado para a las tecnologías ofreciendo un escenario idóneo para su tratamiento en la búsqueda de proporcionar una mayor calidad tanto a la gestión pública como a la vida de cada uno de los venezolanos.

La profesora Mariliana Rico Carrillo justifica el intenso desarrollo legislativo por el marcado “propósito de lograr la actualización de normas y la integración del país en el marco de la economía globalizada” (Rico Carrillo, 2003). Sin embargo, esta labor de creación legislativa no siempre es sencilla y mucho menos fácil, particularmente porque cuando se trata de legislar en materias de tecnologías, en algunos casos cuando las normas promulgadas resultan inaplicables por su obsolescencia, ya que la tecnología a la cual se aplica la regulación se encuentra en desuso.

El autor Rafael Hernando Gamboa Bernate se refiere a esta situación en el marco normativo como “talanqueras”, y lejos de verlas como obstáculos las presenta como retos de investigación, aunque reconoce que

es un hecho irrefutable que la regulación jamás se podrá desarrollar a la misma velocidad que lo hacen las telecomunicaciones. Éstas por su dinamismo y naturaleza, sólo se restringen por la rapidez con que

se desarrollen, sin atender a más criterios que las necesidades de la sociedad y su viabilidad tecnológica. En pocas palabras, la tecnología es el reflejo anticipado de las necesidades sociales. (Gamboa, 2005)

Las normas jurídicas son elaboradas con la intención de que perduren en el tiempo, “hay un afán de perennidad que anima a los legisladores. Están tan convencidos de la bondad de la norma que promulgan y de su adaptabilidad a las necesidades sociales actuales y futuras, que generalmente la dictan “para siempre”. Hacen excepción en esto solamente escasas leyes de carácter temporal, concebidas y destinadas a regir durante un período determinado, comúnmente breve, que ellas mismas señalan” (Novoa, 1979). En el caso de las normas cuya finalidad es la de regular las tecnologías de información y comunicaciones, ciertamente no encuadran en la excepción presentada por el autor citado, ya que no se tratan de normas temporales; por el contrario, se requiere que estas normas perduren el mayor tiempo posible.

El problema de la obsolescencia normativa, causado por la rápida modificación de la tecnología que regula, ha sido resuelto, en teoría, incorporando en los textos legislativos el principio llamado “neutralidad tecnológica”, el cual consiste

en el respeto al uso de cualquier tecnología que se utilice o pueda usarse en el futuro a los efectos de transmitir un mensaje de datos o insertar una firma electrónica, por lo tanto implica no favorecer unas tecnologías sobre otras con la finalidad de evitar posibles obsolescencias legales (Rico Carrillo, 2003).

El autor español Agustín Madrid Parra, al referirse a este principio, plantea que las legislaciones que vienen a regular la materia electrónica tienen la necesidad de establecer su base en determinada tecnología. Lo que se persigue con esta posición neutra es no inclinarse por un concreto método o técnica para llevar a cabo, por ejemplo, la identificación del autor del mensaje de datos (Madrid Parra, 2001).

En este sentido, la norma jurídica de contenido tecnológico debe establecer funciones y requisitos de carácter general puesto que si se hace una opción a una concreta tecnología, el riesgo de obsolescencia en un corto tiempo es muy elevado. Se requiere que la norma jurídica tenga, como ya hemos dicho, vigencia prolongada en el tiempo, de forma que sea posible dar cobertura a futuros instrumentos técnicos cuyo uso se pueda implementar en transacciones de relevancia jurídica.

La reglamentación jurídica de los medios electrónicos de comunicación e información deberá ser susceptible de adaptarse a las situaciones de constantes cambios e innovaciones que caracterizan al sector de la tecnología. Esto favorecería el empleo de una técnica legislativa de cláusulas o principios generales que se traduzca en una regulación siguiendo criterios flexibles, evitando introducir variaciones o reformas en las normas en corto tiempo.

La función que cumplen las normas en el entorno de las tecnologías de información y comunicación es brindar un marco jurídico apropiado para el desarrollo de los Sectores-e; es decir, aquellos sectores en los cuales las tecnologías de información y comunicación han servido para su crecimiento y difusión. En la actualidad se destaca el avance de las tecnologías de información y comunicación tanto en las relaciones públicas como privadas que comprenden relaciones comerciales como no comerciales, es así como se hace referencia a los siguientes sectores: Comercio-e, Gobierno-e, Salud-e, y Enseñanza-e, a lo cual se le debe sumar la necesidad de crear un ambiente de seguridad y confianza en la comunicación digital, ya que las mismas se presentan como elementos claves, especialmente en el caso de la realización de transacciones comerciales con el uso de Internet. Esto ha sido destacado en un informe de la CEPAL del año 2003:

Las cuestiones de seguridad y confianza no son relevantes sólo para los consumidores finales, sino también para las relaciones internas de las organizaciones. En el caso del comercio-e interempresarial (B2B), por ejemplo, la información registrada que se envía a través de las redes, que puede contener secretos comerciales y estrategias de las empresas, podría ser sustraída. Por este motivo, los negocios que expanden sus redes internas para conectarse con otras empresas suelen preocuparse de establecer una firme relación de confianza. Las iniciativas en las áreas de protección al consumidor, como los códigos éticos para la publicidad y las normas de cumplimiento de contratos podrían inspirar la creación de programas formativos para consumidores y empresas sobre los riesgos y los beneficios de realizar transacciones mediante las redes, definir directrices sobre protección del consumidor y animar al sector privado a que adopte las medidas de autorregulación tales como códigos de conducta y programas de confianza empresarial. Naciones Unidas, Comisión Económica Para América Latina y El Caribe-CEPAL, 2003.

Como consecuencia de esta situación, la mayor parte de las referencias legislativas existentes en materia de contratación por medios

electrónicos en el mundo se centran en medidas para garantizar la autenticidad de los datos emitidos a través de medios electrónicos, la intimidad y la confidencialidad de la información personal y empresarial, el reconocimiento de documentos electrónicos, firmas digitales y autoridades de certificación; en el aspecto de la protección se destaca la regulación en torno a los consumidores y usuarios y la estandarización de los delitos electrónicos, tanto los referidos a las personas como a los bienes.

1.- Acerca del Decreto-Ley de Mensajes de Datos y Firmas Electrónicas:

En el caso venezolano, esta tarea ha sido encomendada al Decreto N° 1.204 con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001, el cual tiene por objeto “otorgar y reconocer eficacia y valor jurídico a las firmas electrónicas, a los mensajes de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas”.

Los orígenes de este Decreto-Ley no están claros, ya que por haber sido dictada dentro del conjunto de leyes del marco de la ley habilitante dada al presidente de la república, publicada en la Gaceta Oficial N° 37.077 Ordinaria de fecha 14 de noviembre de 2000, no hay archivos en la Asamblea Nacional sobre sus discusiones. Sin embargo, la doctrina se ha pronunciado en el siguiente sentido:

Ninguna mención se hace de los trabajos de la UNCITRAL o de la Directiva de la Comunidad Europea. El rechazo de estas fuentes o su ignorancia no deja de ser preocupante, porque las leyes modelo de UNCITRAL están acompañadas, cada una de ellas, de una guía para su incorporación en el derecho interno, “con miras a asistir a los poderes ejecutivo, legislativo y judicial”. La comprensión de las normas de las leyes modelo de UNCITRAL se facilita enormemente por unas guías que han sido redactadas en un lenguaje impecable y de modo meticuloso. El desdén por este material de valor internacional no tiene sentido. (Morles Hernández, 2001, p. 13).

En criterio contrario, Rico Carrillo expresa que la Ley sobre Mensajes de Datos y Firmas Electrónicas tiene su origen en los trabajos de la UNCITRAL, específicamente la Ley Modelo sobre Comercio Electrónico y la Ley Modelo sobre Firmas Electrónicas, haciendo la precisión

de que, en el caso venezolano, se ha sistematizado el tratamiento legal de estas dos figuras en un solo cuerpo legislativo. En este sentido, la autora reconoce que la finalidad de este instrumento:

Constituye el punto de partida para la tramitación de los procedimientos electrónicos en el campo de la Administración Pública y la administración de justicia, cabe destacar que los diversos textos jurídicos promulgados luego de la adopción de esta ley, contemplan de una u otra manera la posibilidad de tramitación de los procedimientos tradicionales en forma electrónica (Rico Carrillo, 2003).

No obstante, la discusión sobre el origen del Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas, lo que sí queda meridianamente claro es la incorporación de los principios del desarrollo tecnológico, a saber:

1. **Equivalencia Funcional:** El documento de soporte informático produce los mismos efectos del documento contenido en papel, con la firma autógrafa de su autor.
2. **Neutralidad tecnológica:** La no adhesión a una sola tecnología en las regulaciones.
3. **Imposibilidad de alterar el derecho de preexistente de las obligaciones y contratos:** En los contratos electrónicos los elementos esenciales del negocio jurídico no deben ser modificados, ya que se trata solo de un nuevo medio de representación de la voluntad negocial.
4. **Buena fe en materia de contratación electrónica:** En la utilización de los medios informáticos para la realización de los negocios jurídicos debe existir un alto grado de confianza entre todos los participantes.
5. **Libertad Contractual:** Se representa, por un lado, como la libertad de elección de la forma electrónica para la celebración de negocios jurídicos y, por otro, la libertad de contenido; es decir, la expresión de la autonomía de la voluntad de las partes.

Bajo el imperio de estos principios, el Decreto-Ley bajo análisis incorpora la regulación de los Mensajes de Datos y de las Firmas Electrónicas, y de las figuras que se relacionan a estos, a saber: la Superintendencia de Servicios de Certificación Electrónica, los Proveedores de Servicios de Certificación Electrónica y de los Certificados Electrónicos. En el cuadro a continuación resumimos el tratamiento legal.

ELEMENTOS	TRATAMIENTO
Mensaje de Datos	Definición legal: "Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio."
	Reconocimiento del valor probatorio de los mensajes de datos: "Tendrá la misma eficacia probatoria que la ley otorga a los documentos escritos... Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil."
	Garantía del Derecho a la Privacidad: "Estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal."
	Formalidades: "Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto-Ley."
	Autoría: "Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un Mensaje de Datos al tener asociado una Firma Electrónica."
	Integridad: El Mensaje de Datos podrá ser preservado en su forma original, inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación. Accesibilidad: El Mensaje de Datos debe ser susceptible de ser consultado posteriormente a su creación; estar conservado en el mismo formato que se generó, archivó o recibió o en algún formato que contenga con exactitud la información generada o recibida, y; deberá ser susceptible de determinar su origen y destino, así como, la fecha y hora en que fue enviado o recibido.
ELEMENTOS	TRATAMIENTO
Firmas Electrónicas:	Definición Legal: "Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado."
	Reconocimiento del valor probatorio: La Firma Electrónica que permita atribuir autoría a los Mensajes de Datos tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa.
	Requisitos para la validez y eficacia probatoria: La Firma Electrónica deberá: a) garantizar que los datos utilizados para su generación pueden producirse sólo una vez, y asegurar, razonablemente, la confidencialidad; b) ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento, y; c) no alterar la integridad del Mensaje de Datos.
	Efectos jurídicos: Cuando la Firma Electrónica no cuente con los requisitos para su validez y eficacia probatoria, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.
	Firma Electrónica Certificada: Es aquella que ha sido debidamente certificada por un Proveedor de Servicios de Certificación Electrónica

ELEMENTOS	TRATAMIENTO
<p>Superintendencia de Servicios de Certificación Electrónica (SUSCERTE):</p>	<p>Características: Servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, dependiente del ministerio con competencia en Ciencia y Tecnología.</p>
	<p>Objeto: Acreditar, supervisar y controlar a los Proveedores de Servicios de Certificación Electrónica, públicos o privados.</p>
	<p>Competencias:</p> <ol style="list-style-type: none"> 1) Otorgar la acreditación y renovación a los Proveedores de Servicios de Certificación Electrónica. 2. Revocar o suspender las acreditaciones otorgadas. 3. Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación Electrónica. 4. Verificar que los Proveedores de Servicios de Certificación Electrónica cumplan con los requisitos previstos por la ley. 5. Supervisar las actividades de los Proveedores de Servicios de Certificación Electrónica. 6. Liquidar, recaudar y administrar las tasas establecidas en la ley. 7. Liquidar y recaudar las multas establecidas en la Ley. 8. Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones. 9. Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de la ley. 10. Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación Electrónica. 11. Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativo a las presuntas infracciones de la ley. 12. Requerir a los Proveedores de Servicios de Certificación Electrónica o sus usuarios, cualquier información que considere necesaria y que esté relacionada con las materias de su competencia. 13. Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores de Servicios de Certificación Electrónica y sus usuarios, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a la ley que rige la materia. 14. Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones. 15. Presentar un informe anual sobre su gestión al Ministerio de adscripción. 16. Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en la ley. 17. Imponer las sanciones establecidas en la ley. 18. Determinar la forma y el alcance de los requisitos para la acreditación de los Proveedores de Servicios de Certificación Electrónica. 19. Las demás que establezca la ley y sus reglamentos.

ELEMENTOS	TRATAMIENTO
Proveedores de Servicios de Certificación Electrónica	<p>Definición Legal: "Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley".</p> <p>Requisitos: Personas naturales o jurídicas, públicas o privadas, que cumplan con los siguientes requisitos:</p> <ol style="list-style-type: none"> 1) capacidad económica y financiera suficiente para prestar los servicios autorizados para los Proveedores de Servicios de Certificación Electrónica; 2) capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos; 3) garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro de los Certificados Electrónicos que proporcionen; 4) un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados Electrónicos que hubieren proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos; 5) garantizar que la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales, que estén protegidos contra su alteración o modificación, de tal forma que garanticen la seguridad técnica de los procesos de certificación; 6) en caso de las personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen; 7) personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar y; 8) las demás que señale el reglamento de la ley.
	<p>Actividades:</p> <ol style="list-style-type: none"> 1) proporcionar, revocar o suspender los distintos tipos o clases de Certificados Electrónicos; 2) ofrecer o facilitar los servicios de Firmas Electrónicas; 3) ofrecer servicios de archivo cronológico de las Firmas Electrónicas certificadas por el Proveedor de Servicios de Certificación Electrónica; 4) ofrecer los servicios de archivo y conservación de los Mensajes de Datos; 5) garantizar Certificados Electrónicos proporcionados por Proveedores de Certificados Electrónicos extranjeros, y; 6) las demás que establezca la ley y sus reglamentos.
	<p>Obligaciones:</p> <ol style="list-style-type: none"> 1) adoptar las medidas necesarias para determinar la exactitud de los Certificados Electrónicos que proporcionen y la identidad del Signatario; 2) garantizar la validez, vigencia y legalidad del Certificado Electrónico que proporcione; 3) verificar la información suministrada por el Signatario para la emisión del Certificado Electrónico; 4) mantener en medios electrónicos o magnéticos, para su consulta, por diez (10) años siguientes al vencimiento de los Certificados Electrónicos que nen, un archivo cronológico con la información relacionada con los referidos Certificados Electrónicos;

ELEMENTOS	TRATAMIENTO
<p>Proveedores de Servicios de Certificación Electrónica</p>	<ol style="list-style-type: none"> 5) garantizar a los Signatarios un medio para notificar el uso indebido de sus Firmas Electrónicas; 6) informar a los interesados en sus servicios de certificación, utilizando un lenguaje comprensible en su página en la Internet o en cualquier otra red mundial de acceso público, los términos precisos y condiciones para el uso del Certificado Electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia; 7) garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo confiable y seguro de dicha información; 8) garantizar la adopción de las medidas necesarias para evitar la falsificación de Certificados Electrónicos y de las Firmas Electrónicas que proporcionen; 9) efectuar las notificaciones y publicaciones necesarias para informar a los signatarios y personas interesadas acerca del vencimiento, revocación, suspensión o cancelación de los Certificados Electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con dichos Certificados Electrónicos; 10) notificar a la Superintendencia de Servicios de Certificación Electrónica cuando tenga conocimiento de cualquier hecho que pueda conllevar a su inhabilitación técnica.
	<p>Acreditación de los Proveedores:</p> <p>Definición Legal: "Es el título que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en este Decreto-Ley."</p>
<p>Certificados Electrónicos:</p>	<p>Definición Legal: "Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica."</p>
	<p>Función: Garantiza la autoría de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos.</p>
	<p>Carácter: No confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban.</p>
	<p>Contenido:</p> <ol style="list-style-type: none"> 1) identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica; 2) el código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica; 3) identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica; 4) las fechas de inicio y vencimiento del periodo de vigencia del Certificado Electrónico;

ELEMENTOS	TRATAMIENTO
	5) la Firma Electrónica del Signatario; 6) un serial único de identificación del Certificado Electrónico, y; 7) cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.

Fuente: Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas

Luego en la Gaceta Oficial No. 38.086 de fecha 14 de diciembre de 2004, apareció publicado el Decreto No. 3.335, mediante el cual se dicta el Reglamento Parcial del Decreto Ley sobre Mensaje de Datos y Firmas Electrónicas, el cual tiene como finalidad desarrollar las normas que regulan la acreditación de los Proveedores de Servicios de Certificación Electrónica, y se presenta como una continuación de las disposiciones consagradas en el Decreto-Ley sobre Mensaje de Datos y Firmas Electrónicas del año 2001, estableciendo el procedimiento a seguir por las personas interesadas en prestar servicios de certificación electrónica, también se crea el Registro de Auditores.

3.- Utilización de la Ley de Mensajes de Datos y Firmas Electrónicas en los tribunales venezolanos:

En los primeros diez años de vigencia del Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas, fueron dictadas por los tribunales patrios interesantes decisiones sobre el reconocimiento de éstos como medios de prueba, en las cuales se destacan aspectos tales como el reconocimiento de Internet como medio de realización de actos con relevancia jurídica; el valor probatorio de los mensajes de datos y firmas electrónicas y la equiparación del mensaje de datos impreso a las copias o reproducciones fotostáticas, entre otros, los cuales han sido sintetizados en el siguiente cuadro:

Datos de las sentencias	Elementos de análisis	Consideraciones (Extractos de sentencias)
Sala Constitucional del T.S.J O. Álvarez en Amparo Sentencia del 09/04/2001	Reconocimiento de Internet	Esta Sala por interpretación progresiva del artículo 16 de la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales admite que, dentro del medio telegráfico a que hace alusión dicho articulado, está incluido el Internet como medio posible de interposición de la petición de amparo constitucional, limitándola a casos de urgencia y a su ratificación, personal o mediante apoderado, dentro de los tres (3) días siguientes a su recepción. Ello es así con el fin de no limitar el derecho al

Datos de las sentencias	Elementos de análisis	Consideraciones (Extractos de sentencias)
<p>Sala Constitucional del T.S.J O. Álvarez en Amparo Sentencia del 09/04/2001</p>	<p>Reconocimiento de Internet</p>	<p>acceso a la justicia del accionante, por constituir no sólo un hecho notorio la existencia del Internet como medio novedoso y efectivo de transmisión electrónica de comunicación, sino que, además, dicho medio se encuentra regulado en el ordenamiento jurídico venezolano por el reciente Decreto-Ley N° 1204 sobre Mensajes de Datos y Firmas Electrónicas,...donde se le da inclusive valor probatorio a dichas transmisiones.</p>
<p>Corte Superior del Tribunal de Protección del Niño y del Adolescente del Área Metropolitana de Caracas y Nacional de Adopción Internacional.</p> <p>H.T. Rojas contra R. de Marchena Sentencia del 11/11/2004</p>	<p>Equiparación del Mensaje de Datos impreso a las copias o reproducciones fotostáticas</p>	<p>La Corte Superior no considera que la valoración del mensaje de datos promovido por el demandado reconvincente como documento público o privado sea correcta, ya que carece de firma autógrafa o de firma electrónica. De conformidad con el artículo 4 de la Ley sobre Mensajes de Datos y Firmas Electrónicas su valor, una vez impreso, sería el mismo que la ley le atribuye a las copias o reproducciones fotostáticas.</p>
	<p>Forma de Impugnación</p>	<p>El artículo 429 del Código de Procedimiento Civil establece que las copias o reproducciones fotostáticas se tendrán como fidedignas si no fueren impugnadas por el adversario. En este sentido, la parte contra quien se opone la referida copia del mensaje de datos debió desconocer dicho instrumento de conformidad con el artículo 444 del Código de Procedimiento Civil, no siendo así se tiene por cierto su contenido lo que hace plena prueba de la relación existente entre los ciudadanos.</p>
<p>Sala de Casación Social del Tribunal Supremo de Justicia, caso: Luis Alberto Navas Jiménez contra la sociedad mercantil C.A. VENCEMOS Sentencia del 05/03/2007</p>	<p>La inalterabilidad como requisito del documento electrónico</p>	<p>En el caso de los documentos electrónicos existirán tantos documentos originales como documentos inalterados existan, así lo establece el contenido del artículo 7 de la Ley de Mensajes de Datos y Firmas Electrónicas, ello quiere decir que tanto el documento que viaja por la red, el que está en el disco duro del ordenador o los que están grabados en otro soporte también son originales, siempre que cumplan el requisito de inalteración.</p>
<p>Sala de Casación Civil del Tribunal Supremo de Justicia, caso: Distribuidora Industrial de Materiales C.A. (DIMCA), contra Rockwell Automation de Venezuela, C.A. Sentencia del 24/10/ 2007</p>	<p>Naturaleza y características de los documentos electrónico</p>	<p>El documento electrónico o mensaje de datos es un medio de prueba atípico, cuyo soporte original está contenido en la base de datos de un PC o en el servidor de la empresa y es sobre esto que debe recaer la prueba.</p>

<p>Sala de Casación Civil del Tribunal Supremo de Justicia, caso: Distribuidora Industrial de Materiales C.A. (DIMCA), contra Rockwell Automation de Venezuela, C.A. Sentencia del 24/10/ 2007</p>	<p>Naturaleza y características de los documentos electrónicos</p>	<p>Otra característica del documento electrónico es que éste debe estar conservado en su estado original. En efecto, la Ley de Mensajes de Datos y Firmas Electrónicas exige que cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un mensaje de datos si se ha conservado su integridad y cuando la información contenida en dicho mensaje de datos esté disponible. Para determinar esto, es necesario el examen de un experto a la base de datos del PC o del proveedor de la empresa del cual fue enviado el documento electrónico.</p>
	<p>Prueba de experticia: ¿quién la realiza? y objeto de la experticia.</p>	<p>Los documentos electrónicos no pueden ser exhibidos, por cuanto la manera en la cual son almacenados los datos electrónicos, impide que puedan ser presentados al juicio, pues ellos están en la base de datos de un PC o en el servidor de la empresa, razón por la cual se está frente a la necesidad de una experticia para verificar la autoría de los documentos que se emitan con tales características y si estos están en poder del adversario, hasta tanto se ponga en funcionamiento la Superintendencia de Servicios de Certificación Electrónica.</p>
	<p>Requisito de certificación</p>	<p>En los artículos 20 y 21 de la Ley de Mensaje de Datos y Firmas Electrónicas, crea la Superintendencia de Servicios de Certificación Electrónica, para acreditar, supervisar y controlar a los proveedores de servicios de certificación públicos o privados; inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los proveedores de servicios de certificación y; seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones. Sin embargo, actualmente dicho organismo no está en funcionamiento, razón por la cual hasta tanto se establezca la Superintendencia, debe recurrirse a otro medio de autenticación de los documentos electrónicos, como lo es la experticia.</p> <p>El objeto de esta especial experticia consiste en determinar la autoría del mensaje de datos, esto es, el emisor o la persona autorizada para actuar en su nombre o un sistema de información programado por el emisor o bajo su autorización, para que opere automáticamente y, así saber desde cuál y hacia cuál dirección o puerto electrónico fue enviado y recibido el mensaje;</p>

<p>Sala de Casación Civil del Tribunal Supremo de Justicia, caso: Distribuidora Industrial de Materiales C.A. (DIMCA), contra Rockwell Automation de Venezuela, C.A. Sentencia del 24/10/ 2007</p>	<p>Requisito de certificación</p>	<p>bajo cuál firma electrónica fue enviado; la fecha y hora de la emisión del mensaje; su contenido; y cualquier otro dato de relevancia para el proceso que las partes soliciten o el juez ordene para resolver la controversia.</p> <p>la Sala considera que es necesario certificar si el documento electrónico ha sido conservado y si el mensaje está inalterado desde que se generó o, si por el contrario, ha sufrido algún cambio propio del proceso de comunicación, archivo o presentación, por hechos de la parte o terceros, de conformidad con el artículo 7 de la Ley de Mensajes de Datos y Firmas Electrónicas antes transcrito, lo cual sólo es posible a través de una experticia en la base de datos del PC o el servidor de la empresa que ha remitido el documento electrónico.</p>
<p>Sala Político-Administrativa del Tribunal Supremo de Justicia, con ponencia del Dr. Levis Ignacio Zerpa, caso: PDV-IFT, PDV-INFORMÁTICA Y TELECOMUNICACIONES, S.A., contra INTESA INFORMÁTICA, NEGOCIOS Y TECNOLOGÍA, S.A. y SAIC (BERMUDA) LTD Sentencia del 12/02/2008</p>	<p>Naturaleza jurídica de los documentos electrónicos y consideraciones sobre su valor probatorio</p>	<p>Los Mensajes de Datos formados y transmitidos por medios electrónicos, tendrán la misma eficacia probatoria de los documentos y su promoción, control y contradicción debe atenderse a lo establecido en el artículo 395 del Código de Procedimiento Civil, por remisión del artículo 4 del Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas.</p> <p>Para tramitar la impugnación de la prueba libre promovida, corresponderá al juez emplear analógicamente las reglas previstas en el Código de Procedimiento Civil sobre medios de prueba semejantes, o implementar los mecanismos que considere idóneos en orden a establecer la credibilidad del documento electrónico.</p> <p>La profesora María Inés Arias Ferrer, en un análisis de esta sentencia, establece que la valoración del documento electrónico debe admitir la existencia de distintos tipos de documentos, clasificados a partir de las diversas clases de firmas electrónicas contempladas en la Ley sobre Mensajes de Datos y Firmas Electrónicas, que proveen al documentos distintos niveles de seguridad, tanto en sentido técnico como jurídico, puesto que según el tipo de firma electrónica que se trate será un documento electrónico privado propiamente dicho o un documento electrónico privado emanado de tercero. (Arias Ferrer, 2008).</p>
<p>Sala Político-Administrativa del Tribunal Supremo de Justicia, ISF ALPIZ INTEGRADORES</p>	<p>Mensajes de datos enviados por la Administración Pública</p>	<p>Interpreta la Sala que no todos los mensajes de datos enviados por la Administración por medios electrónicos deben necesariamente contener los requisitos de forma y de fondo de los actos</p>

<p>DE SOLUCIONES FINANCIERAS, C.A., contra la decisión del MINISTRO DE FINANZAS, hoy Ministro del Poder Popular para Economía y Finanzas, respecto al recurso jerárquico incoado por la omisión del Coordinador de Casos Especiales de la Comisión de Administración de Divisas (CADIVI) Sentencia del 02/02/2010</p>		<p>administrativos, debido a que éstos no pueden igualarse a los actos administrativos formales. Se trata entonces de herramientas que desarrollan y sirven de apoyo para mejorar los servicios ofrecidos a los ciudadanos, simplificando los trámites y formalidades de la actividad administrativa, y para que los interesados tengan acceso a la información sobre la gestión pública. (Vid sentencias de esta Sala Nos. 1011 y 1437 del 8 de julio y 8 de octubre de 2009, respectivamente).</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Fuente: Elaboración propia

Como se puede observar, en el escenario legislativo y jurisprudencial venezolano, la incorporación y aceptación de los mensajes de datos y firmas electrónicas como medios de prueba son cada vez mayores, lo cual ha requerido de un entendimiento de estas figuras por parte de los operadores de justicia y de los agentes de la función pública. No obstante, siguen existiendo vacíos en la regulación de ciertos aspectos de las tecnologías, tales como la protección de datos personales en redes o en Internet.

Conclusiones

El poder integrar a un país en la sociedad red no es exclusivamente un problema de tipo tecnológico, tiene que ver con las condiciones económicas, políticas y jurídicas, ya que no se participa de esta sociedad solo teniendo computadoras conectadas ni con un conjunto de normas diseminadas por todo el ordenamiento jurídico sin un hilo conductor que permita su correcta aplicación.

En este sentido, se hace necesaria la evaluación del vigente régimen jurídico de los servicios relacionados con las tecnologías de la información y las comunicaciones, ya que se debe perseguir la competencia y la eficiencia, reconociendo los derechos de los usuarios en las relaciones con relevancia jurídica que se den por medio de la utilización de estas tecnologías y sobre todo debe proponer un catálogo de instrumentos jurídicos que permitan hacer efectivos esos derechos en la esfera jurisdiccional. Esto requiere el conocimiento por parte de todos los operadores y actores del aparato de justicia de los principios que nutren este derecho “tecnológico”.

Si bien para el legislador la regulación de los escenarios digitales resulta en un sistema autónomo dentro del sistema jurídico, no puede dejar de lado a los principios que permitan la incorporación de las tecnologías en todos ámbitos sociales, ya que el desarrollo tecnológico que no se detiene. Por tanto, requerimos cada vez con mayor apremio de jueces y abogados que comprendan el espectro digital donde se desenvuelven los posibles interesados del quehacer jurídico.

Referencias bibliográficas

- Arias Ferrer, M. (2008). La Ley sobre Mensajes de Datos y Firma Electrónica. Comentarios a la Sentencia de fecha 12 de febrero de 2008. *FRONESIS Revista de Filosofía Jurídica, Social y Política*. Instituto Filosofía del Derecho Dr. J. M. Delgado Ocando. Universidad del Zulia. Vol. 15. N° 3.
- Gamboia Bernate, R. (2005). *Soberanía estatal en Internet; análisis desde la perspectiva de conflictos de jurisdicción y competencia en el plano nacional e internacional*. Comercio Electrónico. Legis Editores, S.A. Bogotá, 2005.
- Madrid Parra, A. (2001). Aspectos Jurídicos de la Identificación en el Comercio Electrónico. *Derecho del Comercio Electrónico Primeras*. Jornadas celebradas en la Universidad Carlos III de Madrid. La Ley. Madrid, 2001.
- Morles Hernández, A. (2001). Introducción. *La Regulación del Comercio Electrónico en Venezuela*. Biblioteca de la Academia de Ciencias Políticas y Sociales. Caracas, 2001.
- Naciones Unidas, Comisión Económica Para América Latina y El Caribe – CEPAL. (2003). *Los Caminos hacia una Sociedad de la Información en América Latina y el Caribe*. Conferencia Ministerial Regional Preparatoria de América Latina y el Caribe para la Cumbre Mundial de la Sociedad de la Información. Bávaro, Punta Cana, República Dominicana, 29 al 31 de enero.
- Novoa Monreal, E. (1979). *El Derecho como Obstáculo al Cambio Social*. Siglo XXI Editores, S.A. Tercera Edición. México, 1979.
- Rico Carrillo, M. (2003). *Comercio Electrónico, Internet y Derecho*. Legis Editores, S.A. Primera Edición. Caracas.