Comentarios generales al Decreto-Ley de Mensaje de Datos y Firmas Electrónicas de la República Bolivariana de Venezuela

Andrea Isabel Rondón García*

Resumen

El presente artículo constituye una breve descripción del Decreto-Ley de Mensaje de Datos y Firmas Electrónicas del 28 de febrero de 2001. Para elaborar este artículo hemos considerado pertinente, por una parte, realizar un estudio de la Ley Modelo de la Comisión de las Naciones Unidas sobre el Derecho Mercantil Internacional sobre Firmas Electrónicas y de la Directiva 1999/93/CE de 13 de diciembre de 1999, del Parlamento Europeo y del Consejo de la Comunidad Europea, y por otra parte, consultar doctrina de Argentina y España, pues en estos países desde hace algún tiempo se han venido aplicando estas legislaciones. Nuestro propósito en el presente artículo, luego de consultar el derecho comparado, es analizar una serie de interrogantes y problemas que pudieran suscitarse con la entrada en vigencia de este Decreto-Ley. Finalmente, aun cuando reconocemos que en el Decreto-Ley existen algunos vacíos y resulta difícil su aplicación por nuestros tribunales, considerando su situación actual, no podemos dejar de afirmar que el mismo constituye un importante avance en nuestro ordenamiento jurídico.

Palabras Claves: *Mensaje de datos / Firma electrónica / Documento electrónico / Comercio electrónico / Equivalencia funcional.*

Abstract

This article constitutes a brief description of the Data Messages and Electronic Signatures Act - Decree of February 28th, 2001. In writing this article, we have deemed pertinent, on the one hand, to study the Model Law of the United Nations Commission on International Commercial Law regarding Electronic Signatures and of the Board of Directors 1999/93/CE of December 13th, 1999; of the European Parliament and of the European Community Commission. On the other hand, we considered it relevant to consult the Argentine and Spanish doctrine in view of the fact that for quite some time these countries have been applying these legislations, respectively. The goal of this article, after consulting comparative law, is to analyze a series of issues and problems that could arise with the coming into effect of this Act - Decree. Finally, even though we acknowledge that this Act - Decree contains certain voids and that its application in our courts is difficult, we cannot avoid affirming that it constitutes a great advance in our judicial code.

Keywords: *Data message / Electronic signature / Electronic document / Electronic commerce / Functional equivalency.*

---

* Estudiante de 5to. Año de Derecho de la Escuela de Derecho de la Universidad Central de Venezuela. Pasante de la Sala Plena del Tribunal Supremo de Justicia. Preparadora de Derecho Mercantil I. Ex asistente del Área Jurídica del Comité de Familiares de las Víctimas de Febrero y Marzo de 1989 (Cofavic).

Sumario

Introducción. I. Comercio Electrónico y Firma Electrónica. II. El Decreto-Ley de Mensaje de Datos y Firmas Electrónicas de la República Bolivariana de Venezuela. 1) Principios. 2) Los Mensajes de Datos y su Eficacia Probatoria. 3) El Derecho a la Privacidad y el Derecho de Acceso a la Información Personal. 4) Firmas Electrónicas. Requisitos de creación de la Firma Electrónica. 5) Proveedores de Servicios de Certificación y los Certificados Electrónicos. Contenido del Certificado Electrónico. III. Consideraciones Finales.

Introducción

> Venezuela avanza aceleradamente hacia la actualización en materia de tecnologías de información y de las comunicaciones. En los últimos años esta evolución tecnológica ha revolucionado a nivel mundial las diferentes áreas del conocimiento y de las actividades humanas, fomentando el surgimiento de nuevas formas de trabajar, aprender, comunicarse y celebrar negocios. Al mismo tiempo ha contribuido a borrar fronteras, disminuir el tiempo y acortar las distancias...

De este modo inicia la Exposición de Motivos del Decreto-Ley de Mensaje de Datos y Firmas Electrónicas, publicado en Gaceta Oficial N° 37.148, del 28 de febrero de 2001, siendo el primero en su género en nuestro ordenamiento jurídico.

Obviamente el legislador no ha desestimado los avances y cambios que se han suscitado en las sociedades modernas a raíz del surgimiento de los distintos medios de comunicación. Sólo en Venezuela se ha registrado una cifra de 852 mil internautas, lo cual, además de constituir un 8.5% de los usuarios de Internet en América Latina, representa un aumento de casi 62% respecto del año 2000[1].

Vemos, pues, que para realizar transacciones comerciales no sólo disponemos del teléfono, el fax, o la televisión, pues el comercio electrónico posee otros instrumentos como por ejemplo los pagos electrónicos, los sistemas de transferencia de fondos, los EDI (Electronic Data Inter-

[1] Estas cifras fueron tomadas de la Cámara Venezolano de Comercio Electrónico en www.cavecome.org.ve.

change o intercambio electrónico de datos) e Internet, los cuales han sido considerados por World Trade Organization como los siete medios principales del comercio electrónico (Sarra, 2000: 280).

El uso de los medios de comunicación anteriormente enunciados definitivamente elimina, por una parte, las barreras impuestas por el tiempo y el espacio y, por otra parte, la necesidad del uso de documentos o papeles, lo cual ha hecho que el *comercio electrónico* ofrezca múltiples ventajas para sus usuarios. No obstante, la desaparición de esas barreras plantea algunas interrogantes: ¿en caso de conflictos, cuál sería la jurisdicción competente y cuál la ley aplicable?, además, ¿en los contratos electrónicos, cuándo ocurre la formación del consentimiento y cuándo el perfeccionamiento del contrato?, del mismo modo, ¿si no existe un documento o papel, cómo es posible probar la celebración del contrato?

Frente a estas interrogantes es menester una regulación jurídica al respecto y los Estados no pueden permanecer indiferentes ante esta necesidad. En el presente trabajo, luego de hacer algunas referencias generales al comercio electrónico y a la firma electrónica, analizaremos brevemente algunos aspectos del novísimo Decreto-Ley de Mensaje de Datos y Firmas Electrónicas. Estamos conscientes que cada uno de los tópicos abordados por la ley —contratación electrónica, eficacia probatoria de los mensajes de datos y de la firma electrónica, proveedor de servicios de certificación, los certificados, etc.— constituyen, en sí mismos, temas complejos, y que por lo tanto requieren de un estudio pormenorizado[2].

Sin embargo, advertimos al lector que el propósito del presente artículo es exponer, críticamente en ciertos pasajes, el modo como algunos de estos temas han sido tratados y regulados por el nuevo Decreto-Ley, sin pretender realizar un análisis acabado, definitivo, de las instituciones que incorpora la novísima legislación.

I. El Comercio Electrónico y la Firma Electrónica

El comercio electrónico, en un sentido amplio, abarca todas las transacciones comerciales realizadas a través de medios electrónicos como

[2] Para un estudio más profundo de la Ley de Mensajes de Datos y Firmas Electrónicas recomendamos la obra colectiva titulada *La regulación del comercio electrónico en Venezuela*, publicada por la Academia de Ciencias Políticas y Sociales en el año 2001.

teléfono, el fax, los EDI e Internet. En un sentido más restringido, el comercio electrónico "se desarrolla a través de redes (cerradas y abiertas) mediante la relación oferta y demanda, para lo cual se utilizan herramientas electrónicas y telecomunicaciones" y abarca "todas las formas en que puede desarrollarse el comercio, es decir, entre Estados, entre Estados y empresas, entre Estados y particulares, entre empresas, entre empresas y consumidores y entre consumidores" (Sarra, 2000:279).

De este último concepto vale destacar que el comercio electrónico puede utilizar las redes para transmitir datos en un determinado mercado o que en el comercio electrónico las redes mismas son el mercado. Un ejemplo del primer caso lo constituyen los EDI, los cuales han sido definidos como "la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto"[3]. La Internet constituye un ejemplo del segundo caso, y en ella se distinguen dos modalidades, una de ellas el comercio electrónico directo —se realiza completamente por vía electrónica— y la otra el comercio electrónico indirecto —los pedidos se realizan a través de las redes y el suministro es a través de los medios normales de distribución— (Sarra, 2000:284, 285).

Esta nueva forma de comerciar cada vez es más utilizada por un mayor número de personas que encuentran en ella un sinnúmero de ventajas respecto del comercio tradicional. En efecto, el comercio electrónico ofrece una amplia variedad de bienes y servicios a un amplio número de consumidores, brinda flexibilidad de horarios, permite obtener de forma rápida la información necesaria para comprar, evita tener que desplazarse de un sitio a otro y facilita gozar del anonimato para visitar la tienda (Paz-Ares, 2000:86).

No obstante estas ventajas, el comercio electrónico también trae consigo varios inconvenientes, pues ¿cómo garantizar a los consumidores la protección a la privacidad o a la propiedad intelectual?, ¿cómo sabemos que un contrato se ha perfeccionado?, ¿en caso de conflictos, cuál será la legislación aplicable y cual será la jurisdicción que conocerá del caso? Frente a estos problemas, el Estado no puede permanecer neutral, ni tampoco puede darse a la tarea de sancionar leyes que resulten res-

[3] Definición de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico. El texto completo puede ser consultado en www.uncitral.org.

trictivas, que en lugar de propiciar un clima de seguridad y certeza, constituyan verdaderos obstáculos al comercio electrónico.

En tal sentido, el Estado debe ofrecer un marco legal que brinde seguridad a los usuarios de esta forma de realizar transacciones comerciales, pues ésta es la única vía en que se garantizará el desarrollo del comercio electrónico, el cual, sin lugar a dudas, significa hoy en día una verdadera alternativa para aquellos que deseen ampliar sus relaciones comerciales, expandir su ámbito de acción, desarrollar su actividad económica, etcétera.

Como ya lo hemos advertido, en el comercio electrónico, al igual que las tradicionales barreras impuestas por el tiempo y el espacio, la necesidad del uso del papel ha sido eliminada. Es por esta razón que la *firma electrónica* adquiere una gran importancia, pues, en este campo se habla de documentos electrónicos y es ella misma (la firma electrónica) la que atribuye la autoría a estos documentos.

La Enciclopedia Jurídica Omeba identifica la noción de documento a la noción de instrumento, el cual es "el papel escrito y por lo regular firmado para hacer constar algún hecho o acto" (1977:198). Por su parte Eduardo J. Couture define al documento como un "instrumento; objeto normalmente escrito, en cuyo texto se consigna o representa alguna cosa apta para establecer un hecho o se deja constancia de una manifestación de voluntad que produce efectos jurídicos" (1997:239). De estos conceptos vemos que destaca el elemento de la escritura, y es en este aspecto que el documento electrónico se diferencia del simple documento. En el documento electrónico la declaración se encuentra asentada sobre bits, aquí no existen los trazos manuales que caracterizan al simple documento (Lorenzetti, 2000:62). Para los autores José María Cervelló Grande e Ignacio Fernández, los documentos electrónicos son "aquellos contenidos y almacenados en soportes o equipos informáticos" (Cervelló Grande y Fernández, 2000:393).

Al no poder hablar de firma manuscrita en el comercio electrónico, entonces, comprendemos la importancia que adquiere la firma electrónica, pues es ésta la que garantizará que un documento efectivamente ha emanado de una determinada persona. En este sentido la firma electrónica ha sido definida como "cualquier método o símbolo basado en medios

electrónicos utilizado o adoptado por una parte con la intención de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita" (Martínez Nadal, 2000:38).

Ahora bien, el autor Ricardo Lorenzetti ha señalado que la firma electrónica es el género y la firma digital es la especie, pues, en ésta última, se agregan elementos de seguridad que la firma electrónica no tiene (2000:78). Este autor también ha señalado que "las legislaciones reconocen el género de firma electrónica y luego eligen una especie dentro de él, que denominan "firma electrónica avanzada", o "firma digital", que es la que utiliza un sistema, generalmente criptográfico, que da seguridad" (2000:78).

Sobre el modo en que estos aspectos han sido regulados por el Decreto-Ley de Mensaje de Datos y Firmas Electrónicas de la República Bolivariana de Venezuela, presentaremos algunos comentarios en el siguiente capítulo. De momento, conviene precisar un poco más la terminología empleada por la literatura y marco jurídico del comercio electrónico.

La firma digital está basada en un sistema de criptografía[4] asimétrica, es decir, la persona que emite el mensaje tiene dos claves, una pública —la cual debe ser accesible para todos— y una privada —la cual sólo es conocida por el titular o incluso ni siquiera es conocida por éste y puede acceder a ella a través de un número de identificación personal o, en el mejor de los casos, con el reconocimiento de una huella digital—, con ésta última clave el emisor cifra su mensaje digitalmente y con la clave pública el receptor lo descifra.

En este proceso puede hacerse uso de la función de hash —algoritmo que puede crear o verificar la firma digital—, pues aplicar la criptografía asimétrica a todo el mensaje puede ser costoso. La función de hash se encargará de resumir el mensaje inicial, en este caso, el receptor recibirá el mensaje inicial y un resumen de ese mensaje, también llamado "huella digital" o "compendio", el cual también será cifrado con la clave

[4] Claudia Brizzio, en su obra *La informática en el nuevo Derecho*, publicada por Abeledo-Perrot, Argentina, 2000, p. 88, cita a Carrascosa López, Del Pozo Arranz y Rodríguez Castro, quienes definen la criptografía como "un sistema de codificación de un texto con unas claves confidenciales y de procesos matemáticos complejos (algoritmos), de forma que resulte incomprensible para el tercero que desconozca la clave descodificadora la actuación que restablece el texto a su forma original".

privada. Una vez que el receptor obtiene tanto el mensaje inicial como el resumen debe proceder a verificar la firma. El receptor aplicará la clave pública para descifrar el resumen o hash recibido y aplicará la función de hash sobre el mensaje completo. Si el hash que descifró y recibió el receptor es idéntico al hash obtenido, podrá estar seguro que el mensaje fue efectivamente firmado por el emisor y con ese contenido[5]. Este sistema le brinda a los usuarios una gran seguridad porque, aun cuando la clave pública esté vinculada matemáticamente con la clave privada, ésta no puede ser obtenida o derivada a través de la clave pública.

En virtud del procedimiento anteriormente descrito la firma digital le brinda al receptor la seguridad de que el mensaje fue enviado por el titular de la clave privada, de que el mensaje no ha sido modificado y de que el emisor no podrá negar el hecho de ser el autor de ese mensaje y con ese contenido, es decir, la firma digital le brinda al receptor, lo que el autor Apol-Lónia Martínez Nadal ha llamado autenticación, integridad y no repudiación en origen, respectivamente (2000:42).

Por su parte, el autor Enrique Montagud Castelló le agrega a la lista anterior otro elemento. En efecto, éste considera que además de la autenticación, la integridad y la no repudiación en origen, la firma digital también ofrece la posibilidad de que el mensaje no pueda ser conocido por un tercero, es decir, este sistema de criptografía asimétrica brinda confidencialidad (Montagud Castelló, 2000:266). Valga señalar acá que en el caso de nuestra Ley de Mensaje de Datos y Firmas Electrónicas no se adopta como única modalidad la firma digital, pues se establecen definiciones generales que no sólo hacen admisible el sistema de la firma digital, dejando libertad para emplear otros.

Hemos enfocado nuestra atención en la firma digital porque ella brinda una serie de ventajas que, de manera innegable, le confiere al comercio electrónico seguridad jurídica, en tanto y en cuanto garantiza la autoría, mantiene la confidencialidad del mensaje, posibilita el control de acceso limitado, mantiene la integridad de la información y asegura la validez probatoria y los plenos efectos de la firma escrita (Lorenzetti, 2000:80-81). Respecto de este último punto es conveniente aclarar que la firma digital en modo alguno sustituye a la firma escrita, ambas son distintas, pues

[5] Ponencia de Apol.lónia Martínez Nadal en el marco de las primeras jornadas de Derecho del Comercio Electrónico celebradas en la Universidad Carlos III y publicada por la Ley en 2001.

con el sistema de criptografía asimétrica no sólo se regula la firma sino también el documento electrónico.

Continuando con la explicación del sistema de criptografía asimétrica, debemos señalar que para garantizar a los usuarios seguridad en sus transacciones, es necesario contar con una entidad certificadora, es decir, una persona que asegure el vínculo que existe entre la clave pública y el titular de la clave privada, un ente que garantice que las claves –la pública y la privada– efectivamente corresponden a esa persona. Esta persona encargada de proveer servicios de certificación podrá ser una persona física o jurídica y de naturaleza privada o pública, todo dependerá de la legislación de cada país, pues existen varios sistemas, como son el del libre establecimiento, el condicionado a la obtención previa de una licencia o acreditación y el de la acreditación voluntaria.

En el primero de ellos cualquier persona podrá proporcionar los servicios de certificación; el segundo de ellos sólo las personas que hayan cumplido con determinados requisitos podrán proporcionar los servicios de certificación; por último, la acreditación voluntaria, la cual supone "todo permiso que establezca derechos y obligaciones específicas para la prestación de servicios de certificación, que se concedería, a petición del proveedor de servicios de certificación interesado, por el organismo público o privado encargado del establecimiento y supervisión del cumplimiento de dichos derechos y obligaciones, cuando el proveedor de servicios de certificación no esté habilitado para ejercer los derechos derivados del permiso hasta que haya recaído la decisión positiva de dicho organismo"[6].

Las principales funciones de estas personas, también conocidas como *proveedores de servicios de certificación*, serán las de emitir certificados electrónicos, identificar inequívocamente los certificados y mantener un archivo de todos ellos. Entre los titulares y usuarios de la firma electrónica y el proveedor de servicios se celebra un contrato que genera una serie de obligaciones entre ambas partes, pues el que solicita los servicios tiene la obligación de colaborar e informar, y el proveedor tiene a su vez las obligaciones de informar a los usuarios y de custodiar estos

[6] Cfr. Art. 2, numeral 13, DOL num. 13, de 19 de enero de 2000, esto es, una de las normativas que al efecto ha emitido el Parlamento Europeo y el Consejo de la Unión Europea para establecer el marco comunitario de la firma electrónica.

datos y mantenerlos en la más estricta y absoluta confidencialidad (Lorenzetti, 2000:88). Vemos pues que la firma electrónica por sí sola no brinda la seguridad que puede ofrecer la firma digital, la cual, por las múltiples ventajas que ofrece, constituye una institución regulada en la mayoría de las legislaciones sobre la materia.

Ahora bien, una vez vista la importancia que adquiere la firma electrónica en el comercio electrónico, cabe preguntarse ¿cuál es la eficacia que se le atribuye a la firma electrónica? En este sentido, debemos destacar que actualmente la tendencia es la de equiparar la validez y efectos de la firma electrónica a los de la firma manuscrita, es decir, hoy en día se aplica la regla del equivalente funcional. No obstante, debemos considerar que esta firma electrónica debe cumplir con algunos requisitos, los cuales estarán determinados por la legislación de cada país.

A continuación analizaremos brevemente la situación del comercio electrónico en Venezuela, a la luz del Decreto-Ley de Mensaje de Datos y Firmas Electrónicas.

II. El Decreto-Ley de Mensaje de Datos y Firmas Electrónicas de la República Bolivariana de Venezuela

El 28 de febrero de 2001 fue publicado el Decreto con Fuerza de Ley de Mensaje de Datos y Firmas Electrónicas[7], el cual se encarga de regular lo relativo a firmas electrónicas, mensajes de datos, proveedores de servicios de certificación y certificados electrónicos. Este es el primer Decreto-Ley en su género y su importancia viene dada por el hecho de que en nuestro ordenamiento jurídico son pocos los casos en los cuales el legislador ha considerado los nuevos medios de comunicación[8].

---

[7] La Ley Habilitante fue publicada en G.O. N° 37.076, el 13 de noviembre de 2000 y el decreto-ley de mensajes de datos y firmas electrónicas en G.O. N° 37.148.

[8] Por mencionar un ejemplo, la Sala Constitucional del Tribunal Supremo de Justicia, el 1° de febrero de 2000, modificó el procedimiento de amparo y una de las novedades incluidas fue la forma de realizar la citación del presunto agraviante y la notificación del Ministerio Público, pues la misma puede hacerse a través de boleta, comunicación telefónica, fax, telegrama, correo electrónico, o cualquier otro medio de comunicación interpersonal (Véase al respecto, Rafael Chavero Gazdik, *"El Nuevo Régimen del Amparo Constitucional en Venezuela"*, Editorial Sherwood, Caracas, 2001, p.221). En virtud de lo establecido en el artículo 335 de la Constitución de la República Bolivariana de Venezuela, la referida sentencia es vinculante "para las otras Salas del Tribunal Supremo de Justicia y demás tribunales de la República". Otro ejemplo relevante lo constituye el Decreto N° 825, publicado en la Gaceta Oficial N° 36.955, el cual establece el acceso y el uso de Internet como política prioritaria para el desarrollo

Esta novedad en nuestro Derecho impone un análisis de la misma, así como de sus implicaciones y adaptación respecto del resto del ordenamiento jurídico.

1. Principios

Este Decreto-Ley en su Exposición de Motivos acoge una serie de principios rectores, entre los que destacamos:

a. Eficacia probatoria

Según la ley, los mensajes de datos y firmas electrónicas tendrán el mismo valor probatorio que el atribuido a los instrumentos escritos y para su incorporación en el proceso se aplicará lo dispuesto en el Código de Procedimiento Civil en lo relativo a las pruebas libres. Este principio enunciado por el Decreto-Ley de Mensajes de Datos y Firma Electrónicas se conoce en la doctrina y en otras legislaciones como *regla del equivalente funcional* (Martínez Nadal, 2000:307), la cual no es más que igualar la validez y los efectos de la firma electrónica a los de la firma manuscrita. En el artículo 4 del Decreto-Ley se acoge tal principio al establecer que "Los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos" y en el artículo 16 al establecer que "La firma electrónica que permita vincular al signatario con el mensaje de datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa".

---

cultural, económico, social y político del país. Entre las disposiciones de este Decreto destaca el artículo 5 pues dispone que "El Ministerio de Educación, Cultura y Deportes dictará las directrices tendentes a instruir sobre el uso de Internet, el comercio electrónico, la interrelación y la sociedad del conocimiento. Para la correcta implementación de lo indicado, deberán incluirse estos temas en los planes de mejoramiento profesional del magisterio". Aun cuando es posterior a la entrada en vigencia de la Ley in comento, es necesario destacar una sentencia del 9 de marzo de 2001, de la Sala Constitucional pues se refiere a los requisitos que deben cumplir las acciones de amparo dirigidas a esa Sala a través del correo electrónico. En esta sentencia se declara inadmisible la acción de amparo interpuesta el 9 de julio de 2000 a través de correo electrónico porque, si bien es cierto que la Sala admite dentro del medio telegráfico a que se refiere el artículo 16 de la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales el Internet, "por constituir no sólo un hecho notorio la existencia" de éste "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", no es menos cierto que la acción de amparo debe ser ratificada personalmente o mediante apoderado dentro de los tres días siguientes, requisito que no fue satisfecho en el caso decidido. Por último, es de mencionar igualmente la Ley Especial contra Delitos Informáticos, publicada en G.O. N° 37.313, el 30 de octubre de 2001.

b. Neutralidad tecnológica

Como ya lo habíamos advertido, en el Decreto-Ley no se establece una modalidad determinada para las firmas electrónicas o para los certificados electrónicos. En efecto, en ella ni siquiera se menciona el sistema de criptografía asimétrica, por lo que deja abierta la posibilidad de admitir otras tecnologías. Esto definitivamente constituye una ventaja, pues el legislador, al no inclinarse por una tecnología determinada, no corre el riesgo de que las disposiciones de este Decreto-Ley carezcan de eficacia al aparecer nuevas tecnologías y caducar otras.

c. No discriminación del mensaje de datos firmado electrónicamente

El legislador ha dispuesto que la firma electrónica no será cuestionada por el solo hecho de presentarse bajo la forma de mensaje de datos. En este sentido debemos señalar que si bien es cierto que el Estado tiene la obligación de crear las condiciones necesarias para garantizar a los usuarios del comercio electrónico seguridad y certeza en la realización de sus transacciones, no es menos cierto que el Estado no puede dictar normas que resulten discriminatorias para aquellos que no utilicen los documentos escritos, en estas circunstancias el Estado debe ser neutral[9].

d. Libertad contractual

Las partes podrán decidir si aceptan o no el uso de las firmas electrónicas. Este principio no es más que una consecuencia de la libertad de comercio. Las partes pueden libremente fijar las pautas que regirán sus relaciones comerciales, con la limitación que constituyen las normas de orden público.

[9] El principio de no discriminación cobra plena vigencia con los artículos 6 y 7 de la ley, los cuales disponen lo siguiente: artículo 6: "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" y artículo 7: "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. A tales efectos, se considerará que un mensaje de datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación".

2. Los Mensajes de Datos y su eficacia probatoria

En los capítulos II y III del Decreto-Ley objeto de nuestro estudio, se regula lo referido a los mensajes de datos así como su emisión y recepción. En el artículo 2 del Decreto-Ley se ha definido el mensaje de datos como "Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio".

El mensaje de datos tiene la misma eficacia probatoria que los documentos escritos y su ingreso al proceso se regulará por lo dispuesto en el artículo 4 del Decreto-Ley. Este mensaje de datos debe cumplir con una serie de requisitos que no resultan ser un mero capricho del legislador, sino que están destinados a crear un clima de seguridad y confianza, pues con ellos se puede asegurar la procedencia y la autenticidad del contenido del documento. Estos requisitos tampoco constituyen, en modo alguno, una discriminación porque no se está cuestionando su validez y eficacia por el hecho de ser un documento electrónico, sino que tan sólo se está regulando de manera especial, en atención a su naturaleza electrónica.

El legislador ha establecido algunos requisitos para el mensaje de datos en el caso de requerirse que la información conste por escrito. En efecto, en el artículo 8 del Decreto-Ley se dispone que:

> Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un mensaje de datos, si la información que éste contiene es accesible para su ulterior consulta.
>
> Cuando la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los mensajes de datos, siempre que cumplan las siguientes condiciones:
>
> Que la información que contengan pueda ser consultada posteriormente.
>
> Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.
>
> Que se conserve todo dato que permita determinar el origen y el destino del mensaje de datos, la fecha y la hora en que fue enviado o recibido.

Como vemos estos requisitos están destinados a determinar si el mensaje ha sufrido o no alguna alteración o si proviene efectivamente de una persona determinada, por lo que el mensaje de datos, para ser admitido como prueba y tener la misma eficacia que un documento escrito, no debe generar dudas respecto de su integridad y de su procedencia.

Los mensajes de datos por ser documentos electrónicos deben cumplir con una serie de requisitos para ser admitidos como prueba. En este sentido, los autores José María Cervelló Grande e Ignacio Fernández han indicado que "el documento deberá reunir, para gozar de predicamento jurídico, una serie de elementos determinantes de su autenticidad y de su autoría y, en especial, la firma de quien asume su contenido y la efectividad de su clausulado" (2000:390).

Una forma sencilla de verificar la autoría del documento es con la firma electrónica del mismo, pues se obtendría autenticidad, no repudio de origen, confidencialidad e integridad para el caso en que se acuda al sistema de criptografía asimétrica. Nuestro Decreto-Ley en su artículo 9 establece que las partes podrán acordar el procedimiento para verificar si el mensaje realmente fue enviado por el emisor. No obstante, ante el silencio de las partes, se considerará que el mensaje ha sido enviado por el emisor cuando éste ha sido enviado por el propio emisor, por una persona autorizada para actuar en nombre del emisor o por un sistema de información programado por el emisor o bajo su autorización.

Estos mensajes de datos serán admitidos en el proceso de acuerdo con lo establecido por el Código de Procedimiento Civil en materia de pruebas libres. De conformidad con lo establecido en el artículo 395 del referido texto legal, las pruebas libres deberán promoverse y evacuarse, por analogía, según las reglas previstas para las pruebas semejantes y a falta de esto, según lo dispuesto por el Juez. Como sabemos, nuestro ordenamiento jurídico adopta el principio de la libertad de la prueba, es decir, se admiten todos aquellos medios de prueba que no estén expresamente prohibidos por la ley. En el caso que nos ocupa, el Código de Procedimiento Civil no prevé los documentos electrónicos, pero si éstos resultan pertinentes y lícitos, podrán ser admitidos, por analogía, de acuerdo con el procedimiento previsto para la prueba documental.

Ahora bien, ¿cuál será el valor probatorio que se le otorgará a los documentos electrónicos? De conformidad con el artículo 4 del Decreto-

Ley "Los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos...". Al hacer un recorrido del Decreto-Ley, vemos que en ninguna disposición se especifica si se trata de documentos públicos o privados. En el Decreto-Ley tampoco se menciona la posibilidad que un funcionario de fe pública del documento, por lo que de la sola lectura, podríamos inferir que se trata únicamente de documentos privados. No obstante, en el Decreto-Ley de Registro y del Notariado, en el artículo 74, numeral 18, se indica como una de las atribuciones de los Notarios la de "autenticar firmas autógrafas, electrónicas y huellas digitales", por lo que también habría que incluir a los documentos públicos.

De conformidad con los artículos 1.359 y 1.360 del Código Civil los documentos públicos hacen plena prueba, entre las partes y frente a terceros, de los hechos jurídicos que el funcionario público declara haber efectuado, visto u oído y de la verdad de las declaraciones formuladas por los otorgantes acerca de la realización del hecho jurídico a que se contrae el instrumento. Igualmente, los documentos públicos y privados hacen plena prueba, según el artículo 1.361, de las cosas expresadas de una manera enunciativa y que guardan una relación directa con el acto.

En cuanto a los documentos privados, según el artículo 1.363 *eiusdem*, si los mismos son reconocidos tienen, entre las partes y frente a terceros, "la misma fuerza probatoria en lo que se refiere al hecho material de las declaraciones".

3. Derecho a la privacidad y derecho de acceso a la información personal

El artículo 5 del Decreto-Ley establece que:

> Los mensajes de datos 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.

En esta disposición se establece la obligación del Estado y de los particulares de garantizar, conforme a la Constitución, dos derechos: el derecho a la privacidad y el derecho de acceder a la información personal, ambos de rango constitucional. A continuación explicaremos brevemente cómo se hallan regulados cada uno de estos derechos en nuestro ordenamiento jurídico.

a. El derecho a la privacidad: en este aspecto, la Constitución de 1999 representa un notable avance respecto de la Constitución de 1961, pues en aquella, en su artículo 60, además de reconocer el derecho al honor, a la vida privada y a la intimidad, establece que los mismos constituyen límites al uso de la informática.

En cuanto a la protección legal de este derecho, tenemos que el 16 de diciembre de 1991 se publicó en la Gaceta Oficial N° 34.863 la Ley sobre Protección a la Privacidad de las Comunicaciones, la cual no ha sido derogada por el Código Orgánico Procesal Penal, sino sólo en aquello que no sea contraria al mismo[10]. Esta Ley no constituye en sí una protección de los datos de una persona; sin embargo, de conformidad con el articulo 1, tiene por objeto la protección de "la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas".

También encontramos regulada esta materia en el Código Orgánico Procesal Penal, el cual en los artículos que van del 233 al 236 regula la ocupación e interceptación de correspondencia y comunicaciones. En estos artículos se prevé una serie de reglas dirigidas a los órganos de investigación policial para regular su actuación en la incautación de correspondencia, la interceptación o grabación de conversaciones telefónicas o de otros medios de comunicación necesarios en la investigación. Nuevamente vemos que estas disposiciones legales no están destinadas a la protección de los datos personales o a restringir el uso de la informática en caso de que la misma menoscabe derechos como la privacidad, el honor o la intimidad.

Finalmente, como ya adelantamos *up supra*, también existe el Decreto-Ley Especial contra Delitos Informáticos. Se justifica una breve reseña del misma porque, tal y como lo expresa el artículo 1 del texto legal, "tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnología". En el capítulo III del referido texto legal se tipifican los delitos de violación de la privacidad

[10] Cfr. artículo 516 del Código Orgánico Procesal Penal.

de la data o información de carácter personal, la violación de la privacidad de las comunicaciones y la revelación indebida de data o información de carácter personal.

Vemos que a diferencia de lo que ocurría con la Ley sobre Protección a la Privacidad de las Comunicaciones y con el Código Orgánico Procesal Penal, este Decreto-Ley establece verdaderas disposiciones que protegen directamente los datos o informaciones personales. En este sentido, el artículo 20 dispone que "El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

Finalmente, en cuanto al desarrollo jurisprudencial de este derecho no podemos dejar de mencionar la sentencia de la Sala Político Administrativa de la extinta Corte Suprema de Justicia, del 8 de agosto de 1994, en la cual se declara con lugar la acción de amparo ejercida contra el artículo 31 de la Ley Especial de Protección a los Depositantes y de Regulación de Emergencias en las Instituciones Financieras por constituir el mismo "una amenaza cierta e inminente de lesión de los derechos constitucionales de nuestros representados a la vida privada y a la intimidad, y a la igualdad y prohibición de discriminaciones..."[11].

Aun cuando en la referida sentencia no se trata el tema del derecho a la intimidad y a la vida privada frente al uso del Internet, consideramos oportuno hacer una breve referencia a la misma porque constituye importantes aportes para la regulación de este derecho. En efecto, esta sentencia tiene el mérito de reconocer que el derecho a la privacidad no es absoluto y que puede ser restringido por el Estado, el cual sólo puede hacerlo de forma taxativa e inmutable respetando (I) el principio de legalidad, (II) que tal restricción sea importante para alcanzar los fines del legislador, (II) se establezca un régimen de garantías para los particulares que resulten perjudicados y (IV) que la ley, como única vía para regular los derechos y garantías, indique las razones por las cuales se utiliza la

[11] La sentencia se encuentra transcrita en el libro titulado *El derecho a la intimidad y a la vida privada y su protección frente a las injerencias abusivas o arbitrarias del Estado* de los profesores Allan Brewer-Carias y Carlos Ayala Corao, publicado por Editorial Jurídica Venezolana, Caracas, 1995.

información, la forma en que se utilizará y la finalidad práctica que se pretende alcanzar.

b Derecho de acceso a la información personal: en la Constitución de 1999 se incluye por primera vez el derecho de acceder a los datos personales. El artículo 28 establece que:

> "Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley".
>
> En esta norma no sólo se consagra el derecho a acceder a la información sino también el derecho a solicitar la actualización, corrección, rectificación o destrucción de la misma si estuviera errada o que afectara sus derechos. Además, tal garantía encuentra refuerzo en lo establecido en el artículo 143 del mismo Texto Constitucional.
>
> En los términos transcritos, la precitada norma constitucional consagra entre nosotros la acción de habeas data, la cual es completamente nueva en nuestro ordenamiento jurídico. Frente a la ausencia de textos legales, la jurisprudencia ha tratado de impulsar el desarrollo de tal garantía. En un primer momento fue definida como una especie del género amparo dirigido a tutelar los derechos al honor, reputación, dignidad, propia imagen, vida privada[12]. No obstante, la Sala Constitucional, el 20 de abril de 2001, con ponencia del Magistrado Jesús Eduardo Cabrera, señaló que los derechos que consagra el artículo 28 de la Constitución, algunos crean situaciones jurídicas y otros producen condenas y "El amparo no está destinado a construir, modificar o extinguir derechos", por lo tanto, "el artículo 28 comentado establece derechos que no pueden confundirse con el amparo". En virtud de la referida sentencia, los derechos que están contemplados en el artículo 28, esto es, el acceso a los registros que existen de una persona y el conocer el fin y el uso de tales registros, podrán ser ejercidos mediante acciones autónomas, pero si se impide o

[12] Cfr. Sentencia del 14 de abril de 2000, Caso INSACA, de la Corte Primera de lo Contencioso-Administrativo, con ponencia del Magistrado Carlos Enrique Mouriño Vaquero.

se minimiza el ejercicio de los referidos derechos, se podrá acudir a la acción de amparo.

4. Firmas electrónicas

Como ya lo habíamos advertido, hoy en día la tendencia es equiparar la validez y los efectos de las firmas electrónicas, que cumplan con determinados requisitos, a los de la firma manuscrita. Conforme al artículo 16 de nuestra Ley, la firma electrónica tendrá los mismos efectos que la firma manuscrita cuando satisfaga los siguientes requisitos:

1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez y asegurar, razonablemente, su confidencialidad.

2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.

3. No alterar la integridad del mensaje de datos.

Antes de entrar a analizar cada uno de los requisitos establecidos por el legislador, es pertinente presentar algunas advertencias al lector:

En primer lugar, el legislador venezolano, al momento de redactar la norma, tomó como punto de referencia lo dispuesto en el Real Decreto de España, Ley 14/1999, pues estos requisitos son bastante similares a los establecidos en el artículo 19 del referido texto legal. Para desarrollar este apartado hemos considerado pertinentes los comentarios que la profesora Martínez Nadal ha formulado al respecto (2000:56-61).

En segundo lugar, se ha discutido sobre la confusión que ha producido la redacción del artículo del Real Decreto, pues en el enunciado del mismo se habla de dispositivos seguros de creación de firmas y al verificar el contenido de la norma, algunos requisitos parecen estar dirigidos a los datos de creación de la firma. Veremos a continuación el significado de cada uno de estos términos y cómo el legislador venezolano ha tratado el tema. En este punto es conveniente advertir que los términos *dispositivos de creación* y *dispositivos de verificación*, aun cuando son empleados por el legislador venezolano, él mismo no los define y tampoco la Ley Modelo de la Comisión de Naciones Unidas sobre el Derecho Mercantil Internacional sobre las firmas electrónicas, por lo que decidimos tomar los conceptos

de la Directiva 1999/93/CE, de 13 de diciembre de 1999 (en adelante DOL num. 13, de 19 de enero 2000), la cual es la normativa legal comunitaria, emanada del Parlamento Europeo y del Consejo de la Unión Europea, en materia de firma electrónica y adoptada por España, cuya doctrina ha sido utilizada en el presente artículo.

En tercer lugar, observamos que lo que el legislador venezolano ha considerado como aspectos que debe cubrir la firma electrónica, en realidad se trata de los referidos a la creación de la firma y no a la firma misma. Para explicar este punto hemos considerado conveniente hacerlo a la luz del sistema de criptografía asimétrica por dos razones: (I) el legislador venezolano al momento de redactar la ley no se inclinó por alguna tecnología en particular, por lo que los comentarios de la firma digital pueden adaptarse perfectamente a este texto legal y (II) el sistema de criptografía asimétrica es el más utilizado por las numerosas ventajas que, como antes se indicó, ofrece.

En el caso de la creación de la firma digital se habla de datós de creación de firma, es decir, "datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica" (artículo 2.4 DOL num. 13, de 19 enero 2000) y de datos de verificación de firma, los cuales son "datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica" (artículo 2.7 DOL num. 13, de 19 enero 2000). Los datos de creación son distintos a los dispositivos de creación, pues éstos se definen como "un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma" (artículo 2.5 DOL num. 13, de 19 enero 2000).

Estos datos de creación y de verificación de firmas son las claves públicas y privadas de las cuales ya habíamos hecho referencia, al tratar sobre la firma electrónica y la firma digital. Estas claves deben satisfacer una serie de requisitos, pues deben garantizar que de la firma pública no se deduzca la firma privada, que no sean fácilmente conocidas por el proveedor de software o hardware y reconstruya así el proceso de creación y deben además utilizar adecuados correctores de aleatoriedad que eviten la producción de claves repetidas.

Los requisitos que se establecen en el artículo 16 se refieren a la generación de los datos de la firma y no a la firma misma, pues con esos

requisitos se buscan claves seguras, no previsibles y no repetidas. A continuación examinaremos los requisitos que deben cumplir estos datos de creación:

a) Garantizar que los datos utilizados para su generación puedan producirse sólo una vez y asegurar, razonablemente, su confidencialidad: en este numeral se observan dos requisitos, uno de ellos es que los datos utilizados para crear la firma puedan producirse una vez, es decir, que deben ser únicos. Sólo debe existir una clave privada. Para evitar el problema de que existan varias personas con un mismo par de claves y que una firma pueda ser atribuida a varias personas es necesario un adecuado procedimiento de generación de claves que incluya un elemento de aleatoriedad.

El segundo de los requisitos es "asegurar, razonablemente, su confidencialidad". Varias interpretaciones se han dado al numeral 1 del artículo 19 del Real Decreto, el cual presenta pocas diferencias respecto del numeral 1 del artículo 16. Una de ellas es que mientras se estén utilizando las claves sobre un mensaje electrónico, las mismas deben ser confidenciales. En esta interpretación, estaríamos hablando de los dispositivos de creación y no de los datos de creación. Otra interpretación que se le ha dado a este requisito es que la clave privada debe estar bajo custodia. Sin embargo, para Martínez Nadal la custodia de la clave privada parece estar reflejada en el requisito 3 del art. 19 del Real Decreto el cual establece "que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros". A nuestro juicio, como este requisito no es exigido en el artículo 16, es perfectamente posible que la confidencialidad a la cual se hace referencia es respecto a la custodia de la clave privada.

b) Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento: este requisito parece referirse a que el mensaje firmado electrónicamente no sea objeto de posteriores modificaciones o que a través de firmas previas no pueda obtenerse de forma ilegítima la firma aparentemente válida de un mensaje.

Por otra parte, debemos indicar que con los avances de la tecnología, las claves que parecen seguras hoy en día, mañana no lo serán, por lo que la seguridad resulta ser un término bastante relativo y es así como lo ha

entendido el legislador al incluir frases como "seguridad suficiente" y "tecnología existente en cada momento".

c) No alterar la integridad del mensaje de datos: en este requisito el legislador venezolano ha resultado ser bastante ambiguo, pues no especifica aquello que no debe alterar la integridad del mensaje de datos. Como el enunciado de la norma se refiere a los aspectos que debe cubrir la firma electrónica para gozar de la eficacia de la firma manuscrita, entendemos que se está refiriendo a que la firma no deberá alterar la integridad del mensaje.

Este requisito, más que estar dirigido a la firma, estaría dirigido a los programas que sirven para aplicar los datos de creación de la firma, por lo que éste se orienta a los dispositivos de creación y consiste en la necesidad que al momento de aplicar la clave privada sobre el mensaje éste no resulte alterado.

Aun cuando la firma electrónica no satisfaga estos requisitos y, por lo tanto, no goce de la misma eficacia jurídica que se le atribuye a la firma manuscrita, podrá "constituir un elemento de convicción valorable conforme a las reglas de la sana crítica" (artículo 17)[13].

El legislador ha considerado que los anteriores requisitos quedan satisfechos ante una firma electrónica debidamente certificada por un proveedor de servicios de certificación, por lo que se hace necesario analizar a continuación cómo ha sido regulado este tema en la ley venezolana.

5. Proveedores de servicios de certificación y los certificados electrónicos

En el artículo 2 del Decreto-Ley se define al proveedor de servicios de certificación como "la persona dedicada a proporcionar Certificados Elec-

[13] En nuestro ordenamiento, el sistema de valoración de las pruebas se ciñe principalmente por las reglas de la sana crítica y excepcionalmente por la ley. En este sentido el artículo 507 del Código de Procedimiento Civil establece que "A menos que exista una regla legal expresa para valorar el mérito de la prueba, el Juez deberá apreciarlas según las reglas de la sana crítica". Para E. J. Couture, en su libro *Fundamento del Derecho Procesal Civil*, las reglas de la sana crítica no son más que la conjunción entre las reglas de la lógica y las reglas de la experiencia del juez), de modo que el juez al momento de valorar las pruebas según las reglas de la sana crítica deberá considerar por una parte, los principios de identidad, de no contradicción y del tercero excluido, y, por otra parte, el "conjunto de conclusiones empíricas fundadas sobre la observación de lo que ocurre comúnmente" (Couture, 1997: 402).

trónicos y demás actividades previstas en este Decreto-Ley". Respecto de esta definición observamos que no se especifica de qué persona se trata, por lo que deja abierta la posibilidad de que el proveedor de servicios pueda ser tanto una persona física como jurídica.

También el legislador ha dejado abierta la posibilidad de que el proveedor de servicios pueda ser público o privado. Esta posibilidad no sólo se deduce del artículo en cuestión sino de otros artículos, como por ejemplo la tercera disposición final, la cual establece que "sin limitación de otros que se constituyan, el Estado creará un Proveedor de Servicios de Certificación de carácter público".

Nótese que en la definición del artículo 2 no se han querido limitar las funciones del Proveedor de Servicios al sólo suministro de certificados electrónicos, pues también se encargan de revocar o suspender los distintos tipos de certificados electrónicos, facilitar los servicios de creación de firmas electrónicas, ofrecer servicios de archivos cronológicos de las firmas electrónicas certificadas, brindar servicios de archivo y conservación de mensaje de datos, garantizar los certificados electrónicos proporcionados por proveedores de servicios extranjeros, entre otras funciones (artículo 34).

Otro de los aspectos importantes de los proveedores de servicios de certificación, y que a nuestro juicio fue tratado de una forma bastante ambigua por el legislador, es el relativo a su constitución jurídica. Como ya lo hemos dicho, existen distintas alternativas para la constitución o el establecimiento de los proveedores de servicios, y en este aspecto el legislador no ha sido claro pues establece algunas disposiciones sobre la acreditación, pero no especifica si la misma debe ser obligatoria o no para el proveedor de servicios.

El artículo 48 dispone que serán sancionadas "las personas que presten los servicios de Proveedores de Servicios de Certificación previstos en este Decreto-Ley, sin la acreditación de la Superintendencia de Servicios de Certificación Electrónica, alegando tenerla". Esta disposición nos hubiera aclarado las intenciones del legislador de establecer un sistema de acreditación obligatoria si no terminara con la frase "alegando tenerla", pues con esta expresión el supuesto de hecho de la norma no es no tener la acreditación sino alegar tenerla cuando en realidad no es así. De esta norma se observa claramente que el legislador no está sancionando la

falta de acreditación, sino el alegar tenerla falsamente, por lo que parecería que la misma no constituye un requisito de obligatorio cumplimiento.

Sin embargo, una lectura de la exposición de motivos de la ley nos orienta en otro sentido. En efecto, en ella se indica que "estos Proveedores de Servicios de Certificación *una vez acreditados*, tendrán entre sus funciones emitir un documento contentivo de información cerciorada que vincule a una persona natural o jurídica y confirme su identidad, con la finalidad que el receptor pueda asociar inequívocamente la firma electrónica del mensaje a un emisor" (el subrayado es nuestro).

Pareciera ser que la intención del legislador era la de establecer un sistema de acreditación obligatoria para poder prestar servicios de certificación, pues además de lo señalado en la Exposición de Motivos, conforme al artículo 21 de la ley se ha de crear la Superintendencia de Servicios de Certificación Electrónica, cuyo objeto será "acreditar, supervisar y controlar (...) a los Proveedores de Servicios de Certificación públicos o privados". No obstante, no basta con que esta intención se observe en la exposición de motivos o se infiera de la lectura de algunas normas, pues la misma debió reflejarse en una disposición que no ofreciera dudas al respecto. Este punto, definitivamente, no queda resuelto.

Ahora bien, una de las funciones del Proveedor de Servicios de Certificación es la de proporcionar los distintos tipos de certificados electrónicos, los cuales han sido definidos en el artículo 2 como mensajes de datos otorgados por el Proveedor de Servicios de Certificación que le atribuyen "certeza y validez a la Firma Electrónica" (artículo 2).

No pareciera quedar clara cuál es la función de los certificados cuando en la definición legal se señala que los mismos confieren certeza y validez a la firma electrónica. Con las palabras "certeza y validez" consideramos que el Decreto-Ley se refiere a que el certificado es el que vincula la firma electrónica con una persona determinada. Esta conclusión es confirmada con el contenido del artículo 38 el cual establece que el "Certificado electrónico garantiza la autoría de la firma electrónica que certifica así como la integridad del mensaje de datos". Vemos pues que el certificado además de vincular una firma con una persona determinada también se encarga de garantizar que el mensaje de datos no ha sufrido alteración alguna.

Otra de las funciones de los proveedores de servicios es la de garantizar que los certificados electrónicos extranjeros cumplen con los requisitos de seguridad, validez y vigencia exigidos por el Decreto-Ley. Este certificado extranjero garantizado por un proveedor de servicios, debidamente acreditado, le proporcionará a la firma electrónica la misma validez y eficacia probatoria que se le otorga a la firma autógrafa. No obstante, si este certificado extranjero no está garantizado por un proveedor de servicios, no le brindará estos mismos efectos a la firma electrónica, sino que la misma constituirá un elemento de convicción valorable según las reglas de la sana crítica (artículo 44).

En cuanto al contenido de los certificados, éstos deberán contener:

a) Identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica: el legislador dejó abierta la posibilidad de que el Proveedor de Servicios fuera una persona física o jurídica, por lo tanto, si trata de una persona jurídica deberá indicar, además de su domicilio y dirección electrónica, su razón social y los datos del registro.

b) El código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica: la Superintendencia será un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión adscrita al Ministerio de Ciencia y Tecnología. Vemos que su creación es importante porque se encargará de certificar a las entidades de certificación y aunque en un principio sea difícil establecerla inmediatamente, se hace necesaria a largo plazo para garantizar el buen funcionamiento (Martínez Nadal, 2000:86).

Para cumplir con este requisito se ha previsto que una de las competencias de la Superintendencia sea la de "mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación públicos o privados" (artículo 22, numeral 3).

c) Identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica: El Decreto-Ley define al signatario como "la persona titular de una Firma Electrónica o Certificado Electrónico" (artículo 2). El legislador, como en el caso de los proveedores de servicios de certificación, deja abierta la posibilidad de que el signatario sea una persona física o jurídica.

d) Las fechas de inicio y vencimiento del período de vigencia del Certificado Electrónico: obviamente, el certificado no puede tener una vigencia indefinida, por lo cual el proveedor de servicios y el signatario deberán acordar el período durante el cual el certificado tendrá vigencia. No obstante la vigencia que puedan acordar el proveedor de servicios y el signatario, éste último podrá solicitar la cancelación o suspensión temporal del certificado.

Conforme al artículo 42 del Decreto-Ley, también se podrá suspender o revocar el certificado cuando sea solicitado por una autoridad competente, se compruebe que los datos del certificado o alguno de ellos proporcionado por el proveedor de servicios son falsos, se compruebe el incumplimiento de alguna de las obligaciones derivadas del contrato celebrado entre el proveedor de servicios y el signatario, se produzca la quiebra técnica del sistema de seguridad del proveedor de servicios que afecte la integridad y confiabilidad del certificado o por incapacidad absoluta del signatario.

e) La firma electrónica del Signatario: Como ya lo advirtiéramos en el punto c, el signatario puede ser una persona natural o jurídica, y en este último caso, se trata de la firma de una persona física con poder de representación, circunstancia que puede hacerse constar en el mismo documento que se firma (Martínez Nadal, 2000: 95).

f) Un serial único de identificación del Certificado Electrónico: este serial único le facilita a los proveedores de servicios el cumplimiento conforme al artículo 35.9 del Decreto-Ley de una de sus obligaciones, a saber, la de "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".

g) Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico: el legislador ha previsto la posibilidad de que los prestadores de servicios puedan limitar su responsabilidad, es decir, no se hará responsable por los certificados que han sido utilizados de forma distinta a la prevista en el certificado y dicho límite debe estar claramente formulado. En este punto es necesario hacer referencia a la responsabilidad de los prestadores de servicios de certificación.

Debemos señalar que nos sorprende que el legislador tratara el tema en la Exposición de Motivos y no en alguna disposición del Decreto-ley. El legislador al explicar los principios que se adoptaban en el Decreto-Ley indica, entre otros, el de la responsabilidad, según el cual "Se excluye la responsabilidad siempre que el sujeto pueda demostrar que ha tomado las diligencias necesarias según las circunstancias. Los Proveedores de Servicios de Certificación Electrónica pueden limitar su responsabilidad, incluyendo en los certificados que emitan las restricciones, condiciones y límites establecidos para su utilización". La Exposición de Motivos, a juicio de la Sala Constitucional, con ponencia del Magistrado Jesús Eduardo Cabrera, el 6 de febrero de 2001, "se consulta sólo a título referencial e ilustrativo para el análisis de la norma constitucional", pues la misma "constituye un documento independiente al Texto Constitucional propiamente dicho y, no siendo parte integrante de la Constitución, no posee carácter normativo", por lo tanto, este aspecto debe ser complementado con las disposiciones del Código Civil y de la Ley de Protección al Consumidor.

Finalmente, para evitar los daños y perjuicios que pueda ocasionar el cese de actividades por parte del proveedor de servicios, el legislador le ha impuesto a éste una serie de obligaciones. El proveedor deberá notificar a la Superintendencia con al menos treinta (30) días de anticipación de su decisión y, en caso de inhabilitación técnica, la notificación deberá ser inmediata.

Luego de estas notificaciones la Superintendencia a través de un acto administrativo declarará públicamente la cesación de actividades del proveedor. La Superintendencia, en virtud de las atribuciones que ejerce, como por ejemplo, supervisar las actividades de los proveedores, inspeccionar y fiscalizar las instalaciones, operaciones y prestación de servicios de los proveedores y solicitarle a los proveedores cualquier información que considere necesaria, podrá investigar los motivos que dieron lugar a la cesación de actividades y adoptar las medidas necesarias que tiendan a proteger a los usuarios.

III. Consideraciones finales

Los nuevos avances tecnológicos nos ofrecen un considerable número de ventajas que nos facilitan la vida, pero ese advenimiento tecnológico

también trae consigo complejidades que no pueden ser subestimadas y que, por el contrario, deben ser consideradas en todo momento por los Estados que, ante este panorama, no pueden permanecer de manos cruzadas.

En el ámbito del comercio electrónico los Estados deben crear las condiciones necesarias de seguridad y confianza para que el mismo se consolide. En el caso específico de Venezuela ya se han dado algunos pasos con el Decreto N° 825, el cual declara el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político del país y con el Decreto-Ley N° 1.204 de Mensaje de Datos y Firmas Electrónicas.

En cuanto a este último instrumento legal, hemos visto que el mismo constituye un avance en nuestro ordenamiento jurídico, por una parte, porque es el primer Decreto-Ley que regula este campo, y, por otra parte, nos revela que las iniciativas legislativas están concientes de la nueva realidad producto de los avances tecnológicos. No obstante, como señalamos a lo largo de este trabajo, la ley presenta algunas deficiencias que deberán ser consideradas en un futuro por el juez mercantil.

Por otra parte, no pretendemos decir que la sola ley será suficiente para regular este campo del comercio electrónico. Además de este Decreto-Ley de Mensajes de Datos y Firmas Electrónicas, es necesario que las futuras iniciativas legislativas consideren otros aspectos que trae consigo el comercio electrónico, por ejemplo la protección de los consumidores, la protección de la propiedad industrial e intelectual, la tributación en Internet, etc.

También se hace necesario preparar a nuestra sociedad para ello. Una parte de este trabajo ya está siendo adelantado pues en el Decreto N° 825 se dispone que "Los medios de comunicación del Estado deberán promover y divulgar información referente al uso de Internet. Se exhorta a los medios de comunicación privados a colaborar con la referida labor informativa", "El Ministerio de Educación, Cultura y Deportes dictará las directrices tendentes a instruir sobre el uso de Internet, el comercio electrónico, la interrelación y la sociedad del conocimiento", "El Ejecutivo Nacional establecerá políticas tendentes a la promoción y masificación del uso de Internet. Asimismo, incentivará políticas favorables para la adquisición de equipos terminales por parte de la ciudadanía, con el objeto

de propiciar el acceso a Internet", entre otras medidas, pero éstas deben acompañarse con iniciativas de las Facultades de Derecho de las distintas universidades del país.

Para finalizar, podemos señalar que la Ley de Mensajes de Datos y Firmas Electrónicas constituye un verdadero avance en nuestro ordenamiento, pero, al mismo tiempo que hacemos esta afirmación, también decimos que este avance representa sólo un pequeño paso para crear un marco jurídico ideal para el desarrollo y la consolidación del comercio electrónico en Venezuela. El trabajo para lograr esto ya ha sido iniciado por el legislador, pero debe ser continuado por los estudiosos del Derecho y de la Informática en forma conjunta.

Bibliografía

Brewer-Carías, Allan y Ayala Corao, Carlos (1995). *El derecho a la intimidad y a la vida privada y su protección frente a las injerencias abusivas o arbitrarias del Estado.* Editorial Jurídica Venezolana, Venezuela.

Couture, Eduardo(1997). *Vocabulario Jurídico.* Ediciones Depalma. Argentina.

Couture, Eduardo (1997). *Fundamento del Derecho Procesal Civil.* Ediciones Depalma, Argentina.

Chavero Gazdik, Rafael (2001). *El nuevo régimen del amparo constitucional en Venezuela.* Editorial Sherwood. Venezuela.

De Miguel Asensio, Pedro Alberto (2001). *Derecho Privado de Internet.* CIVITAS. España.

Enciclopedia Jurídica OMEBA (1977). Tomo XVI. Editorial Bibliográfica Omeba. Argentina.

Henríquez La Roche, Ricardo (1996). *Código de Procedimiento Civil.* Centro de Estudios Jurídicos del Zulia. Venezuela.

Lorenzetti, Ricardo (2000). *Comercio Electrónico.* Abeledo-Perrot. Argentina.

Martínez Nadal, Apol-lónia (2000). *La ley de firma electrónica.* CIVITAS. España.

Martínez Nadal, Apol-lónia (2001). "La Ley española de firma electrónica RDLey 14/1999" en Ramos Herranz, Isabel (Coordinadora) *Derecho del Comercio Electrónico.* La Ley. España.

Paz-Ares, Cándido (2000). "El Comercio Electrónico (Una breve reflexión de política legislativa)". Montagud Castelló, Enrique (2000). "Eficacia jurídica de la firma electrónica". Cervelló Grande, José María y Fernández, Ignacio (2000). "La prueba y el documento electrónico" en DE ROS, Rafael y Juan Manuel Cendoya Méndez De Vigo (Coordinadores) *Derecho de Internet*. Aranzadi Editorial. España.

Sarra, Andrea Viviana (2000). *Comercio Electrónico y Derecho*. Editorial Astrea. Argentina.