XII Jornada Notarial Iberoamericana (II) *

Tema II
Informática Jurídica del Derecho Notarial y del Derecho Registral

A) DOCUMENTO NOTARIAL EN SOPORTE ELECTRÓNICO COMO MEDIO DE AGILIZAR LAS RELACIONES JURÍDICAS TRANSACCIONALES Y SU ACCESO A LOS REGISTROS PÚBLICOS
B) AUTORIDAD CERTIFICANTE

Coordinadora nacional: Escribana Ana María Kemper.

Autores: Escribanos Mauricio Devoto, Gastón Bavera, Hernán Gervasutti, Ángel Francisco Cerávolo, Jorge De Bártolo, Flora M. Katz, Lorena Berutti, María José Pérez Clouet, María Angélica Vitale, Martín Giralt Font, Arnaldo Dárdano, Ana María Kemper, doctor Juan Teodoro Herrmann.

Colaboradora edición: Escribana Patricia A. Lanzón.

---

* Punta del Este (Uruguay), 7 al 10 de noviembre de 2006.

N. de R.: La primera parte de este trabajo se publicó en *Revista del Notariado 887,* p. 75. La tercera y última parte se publicará en el próximo número.

Normativa argentina

Aparición y desarrollo de la firma digital en el campo jurídico de la República Argentina

Ley 25.506/2001
Decreto 2628/2002
Decreto 724/2006

Análisis formativo de la ley 25.506/2001 de firma digital

Desde hace casi diez años la República Argentina cuenta entre su normativa jurídica con la implementación de la técnica de firma digital. Fue por el año mil novecientos noventa y siete, con la aparición de la Resolución número 45, que establecía las pautas para elaborar una normativa sobre firma digital, por lo que en el año mil novecientos noventa y ocho se llegó a la sanción del decreto número 427. Dicha norma, pionera tanto en el orden nacional como internacional, establecía un reconocimiento con validez jurídica para la firma digital, es decir que le otorgaba los mismos efectos que la firma ológrafa, aunque sólo aplicable para el ámbito del sector público nacional. Durante el transcurso de los años se sucedieron varias normas, pero todas restringidas a la órbita del sector público. Fue recién con la sanción de la ley 25.506, en noviembre del año dos mil uno, que se estableció una infraestructura de firma digital de alcance federal, reconociendo la eficacia jurídica tanto de la firma electrónica como de la digital. Luego, en diciembre de dos mil dos, llegó la reglamentación a la ley 25.506 de firma digital, mediante el decreto número 2628, que creó el Ente Administrador de Firmas Digitales y reconoció la certificación digital de documentos electrónicos. Cabe destacar que en la actualidad son varias las provincias argentinas que se han adherido a la ley de firma digital poniéndola en efectivo funcionamiento; pueden señalarse las provincias de La Pampa, mediante la sanción de la ley 2073 del año dos mil tres; Tucumán, mediante la sanción de la ley 7291 del año dos mil tres; Mendoza, con la ley 7234 del año dos mil cuatro; Jujuy, con la ley 5425 y Formosa, con la ley 1454, ambas del año dos mil cuatro; Santa Fe, con la ley 12491 del año dos mil cinco, entre otras.

La ley de firma digital, sancionada por el Congreso el 14 de noviembre de dos mil uno y promulgada de hecho el 11 de diciembre del mismo año, se divide en once capítulos y con un total de cincuenta y tres artículos. Dicha ley es de suma importancia al establecer una clara infraestructura para la implementación de la firma digital en el ámbito federal.

Entre los puntos de mayor importancia cabe destacar el reconocimiento del empleo de la firma electrónica y de la firma digital, destacando su eficacia jurídica, siempre que se cumpla con las condiciones establecidas.

El artículo segundo de la mencionada ley establece el concepto de firma digital, determinando que esta es el resultado de la aplicación de un procedi-

miento matemático de exclusivo conocimiento del firmante y bajo su absoluto control, a un documento digital. Dicha firma digital debe ser susceptible de verificación por terceras partes, permitiendo así identificar al firmante y detectar cualquier tipo de alteración que pudo haber sufrido el documento digital luego de su firma.

Se equiparan los efectos de la firma ológrafa a los de la firma digital, con la salvedad de las disposiciones por causa de muerte, los actos jurídicos del derecho de familia, los actos personalísimos y finalmente aquellos actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, exigidas por la ley o por acuerdo de partes. Por lo que claramente, en el ámbito notarial, las escrituras públicas no pueden ser suscriptas mediante firma digital, sin que les sea de aplicación la presente ley.

El artículo quinto conceptúa la firma electrónica, estableciendo que esta consiste en un conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, que son utilizados por el autor del documento como su medio de identificación, careciendo de alguno de los requisitos específicos establecidos por la ley para configurar una firma digital. Con lo cual no cuenta con presunción de autoría, y para el caso de desconocimiento de la firma electrónica, debe probarse su validez.

Entre los conceptos vertidos por esta ley encontramos el de documento digital: establecido como la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Reglamentando que un documento digital satisface el requisito de la escritura.

Los artículos siete y ocho son de suma importancia por cuanto establecen las presunciones *iuris tantum* de autoría e integridad de aquellos documentos firmados digitalmente. Es decir que se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma. Y en lo que se refiere a la integridad del documento digital, establece que este no ha sido modificado si el procedimiento de verificación de la firma digital aplicado al documento ha sido validado.

La ley en análisis enumera los requisitos necesarios para la validez de una firma digital, a saber: 1) que haya sido creada durante el período de vigencia del certificado digital válido del firmante; 2) haber dado cumplimiento a los requisitos establecidos en el procedimiento de solicitud del certificado, para poder ser verificada; 3) que el certificado haya sido emitido o reconocido por un certificador licenciado.

Otros puntos a destacar de la presente ley se refieren al tema del documento original y al de la conservación de los documentos. El artículo once menciona que "los documentos electrónicos firmados digitalmente y los reproducidos en formato digital, firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales", acarreando su mismo valor probatorio. En cuanto a la conservación de documentos, registros o datos, el artículo doce la establece como exigencia legal, pudiendo utilizar para ello cualquiera de los métodos reglamentados, los cua-

les deberán permitir su accesibilidad, para su posterior consulta, detallando "el origen, destino, fecha y hora de su generación, envío y/o recepción".

En el capítulo dos, la ley define los Certificados Digitales, los cuales consisten en documentos digitales, firmados digitalmente por un certificador, y que vinculan los datos de verificación de la firma con su titular. Para que dichos certificados sean válidos es necesario que el certificador haya sido previamente licenciado por el Ente Licenciante y, además, debe responder a los estándares internacionales fijados por la Autoridad de Aplicación, que en la República Argentina es la Jefatura de Gabinete de Ministros. Todos los certificados digitales tienen un período limitado de vigencia, por lo que la fecha de vencimiento debe ser publicitada y esta nunca podrá ser posterior a la del certificado digital del certificador licenciado que la emitió. En el aspecto internacional, se reconocen certificados extranjeros, siempre previo acuerdo de reciprocidad entre la Argentina y el país de origen del certificador extranjero, además este debe ser a su vez reconocido por un certificador licenciado en el país.

El capítulo tres describe la figura del certificador licenciado, sus funciones, obligaciones, obtención de la licencia y su cese. Será el Ente Licenciante el que otorgue la calidad de Certificador Licenciado; la ley establece que sólo podrán serlo las personas de existencia ideal, registros públicos de contratos u otros organismos públicos. Una vez otorgada la licencia, podrán actuar como proveedores de servicios de certificación. Esta figura también podrá ser utilizada por las entidades que controlan las matrículas de servicios profesionales, de acuerdo con lo establecido por el artículo dieciocho.

En los artículos veinticuatro y veinticinco, se enumeran en forma detallada los derechos y obligaciones que corresponden a todos los titulares de un certificado digital, destacando el derecho a la información y a la confidencialidad.

Los capítulos cinco, seis, siete y ocho establecen cuáles serán los organismos encargados de llevar adelante esta infraestructura de Firma Digital de alcance federal. Entre ellos encontramos: 1) La Autoridad de Aplicación estará a cargo de la Jefatura de Gabinete de Ministros, la cual estará facultada a establecer las normas y procedimientos técnicos necesarios para la correcta implementación de la presente ley. 2) La Comisión Asesora para la Infraestructura de Firma Digital funcionará en el ámbito de la Jefatura de Gabinete de Ministros y emitirá recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la infraestructura de firma digital. 3) El Ente Administrador de Firma Digital, que es el órgano técnico administrativo encargado de otorgar licencias a los certificadores y supervisar su actividad. 4) El Sistema de Auditoría, a cargo de la Sindicatura General de la Nación, evaluará la confidencialidad y la calidad de los sistemas utilizados por los certificadores licenciados.

Asimismo, la ley establece las responsabilidades de todos los entes involucrados y las sanciones que les cabrían para el caso de incumplimiento.

De acuerdo con el artículo cuarenta y nueve de la ley 25.506, el Poder Ejecutivo de la Nación debía proceder a dictar la reglamentación para llevar adelante los objetivos planteados, es por ello que en diciembre de dos mil dos se firmó el decreto 2628. Dicho decreto regula el empleo tanto de la firma elec-

trónica como de la firma digital, los sistemas de comprobación y autoría, la validez y efectos de los certificados que sean emitidos tanto por certificadores licenciados como por los que no lo sean.

La autoridad de aplicación, como se mencionó *ut supra,* será la Jefatura de Gabinete de Ministros, quien llevará una actividad de suma importancia, ya que determinará las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación de documentos con firma digital y/ o electrónica.

Se crea el Ente Administrador de Firma Digital, que actuará bajo la órbita de la Jefatura de Gabinete de Ministros. Será exclusivamente un órgano técnico-administrativo y se encargará de otorgar las licencias a los certificadores y supervisará sus actividades. Asimismo, dictará normas tendientes a asegurar la libre competencia, así como el equilibrio en la participación dentro del mercado de todos los prestadores y protegerá a la parte más débil de la cadena, los usuarios.

Los últimos capítulos del decreto regulan, en primer lugar, el sistema de auditoría; luego tratan sobre la revocación de los certificados digitales; la obtención, efectos, duración y caducidad de los Certificadores Licenciados y, por último, mencionan las funciones de las Autoridades de Registro.

Bibliografía

"Firma Electrónica". María José Ruiz Lancina, Licenciada en Derecho y Doctorado en el Departamento de Derecho de la Empresa de la Facultad de Derecho de la Universidad de Zaragoza, España.

"Mendoza: se lanzó la firma digital". Pablo Mancini, *Cultura Digital* de fecha 22 de noviembre de 2004.

"Firma Electrónica". Leire Sainz de la Maza, Licenciada en Derecho. Especialista en Nuevas Tecnologías.

"Criptografía IX". Luciano Moreno, del Departamento de Diseño web de BJS Software.

"Trabajo sobre firma digital". Notario Carlos Agustín Sáenz, Secretario de Informática del Colegio de Escribanos de la Provincia de Buenos Aires.

Página web: www.pki.gov.ar de la Jefatura de Gabinetes de Ministros, Subsecretaría de Gestión Pública de la Nación Argentina.

Decreto 724/2006 FIRMA DIGITAL. Modifícase la reglamentación de la ley Nº 25.506

Bs. As., 8/6/2006 Publicación en B. O.: 13/6/06

Texto completo

VISTO la Ley Nº 25.506 y el Decreto Nº 2628 del 19 de diciembre de 2002, modificado por el Decreto Nº 1028 del 6 de noviembre de 2003, y CONSIDERANDO:

Que la Ley Nº 25.506 de Firma Digital reconoce la eficacia jurídica del empleo del documento electrónico, la firma electrónica y la firma digital.

Que el Decreto Nº 2628/02 reglamentario de la Ley antes mencionada, establece las condiciones que deben cumplir a tal fin los certificadores que soliciten una licencia.

Que entre dichas condiciones se encuentra la de contar con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los requisitos establecidos en el mencionado decreto.

Que a fin de eliminar condiciones que resulten gravosas sobre la actividad de certificación, considerando especialmente que se trata de un área de reciente desarrollo, resulta conveniente derogar el artículo 30 del mencionado Decreto.

Que asimismo, el mencionado Decreto contiene disposiciones de aplicación específica a la Administración Pública Nacional, entre las cuales se encuentra la de aceptar en sus aplicaciones certificados digitales de certificadores públicos y privados.

Que en virtud de las capacidades desarrolladas por la propia Administración Pública Nacional en materia de firma digital y con el fin de evitar que se encarezcan innecesariamente las tramitaciones que efectúe la comunidad ante al Estado, resulta conveniente la utilización de certificados emitidos por certificadores licenciados públicos en forma gratuita.

Que conforme surge de la facultad contenida en el artículo 52 de la ley 25.506 se procede a actualizar los contenidos del anexo I correspondiente a dicha normativa definiendo el alcance del término "Tercero Usuario".

Que el artículo 23 de la Ley Nº 25.506 de Firma Digital establece el desconocimiento de la validez de un certificado digital si es utilizado para alguna finalidad diferente para la cual fue expedido.

Que en virtud de ello, el tercero usuario tiene derecho a aceptar o rechazar documentos electrónicos firmados digitalmente utilizando certificados cuya política de certificación no reúna las condiciones por él requeridas.

Que a fin de adecuar el decreto reglamentario al espíritu de la Ley 25.506, se considera conveniente modificar su artículo 1º inciso b), reconociendo que los certificados digitales emitidos por certificadores no licenciados permiten verificar firmas electrónicas.

Que ha tomado intervención el servicio jurídico permanente de la jurisdicción.

Que la presente medida se dicta en virtud de lo dispuesto por el artículo 99, inciso 2, de la Constitución de la Nación Argentina.

Por ello, ***EL PRESIDENTE DE LA NACIÓN ARGENTINA DECRETA:***

Artículo 1º – *Derógase el artículo 30 del Decreto Nº 2628 del 19 de diciembre de 2002.*

Art. 2º – *Sustitúyese el texto del artículo 38 del Decreto Nº 2628 del 19 de diciembre de 2002 por el siguiente: "Artículo 38. Las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional podrán ser certificadores licenciados y emitir certificados para agentes y funcionarios públicos y particulares, tanto sean personas físicas como jurídicas. Dichos certificados deberán ser provistos en forma gratuita.*

En aquellas aplicaciones en las que la Administración Pública Nacional interactúe con la comunidad, solamente se admitirá la recepción de documentos digitales firmados digitalmente utilizando certificados emitidos por certificadores licenciados o certificados extranjeros reconocidos en los términos del artículo 16 de Ley 25.506".

Art. 3º – *Incorpórase al Anexo I del Decreto Nº 2628 del 19 de diciembre de 2002, la siguiente definición: "18. TERCERO USUARIO: persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente".*

Art. 4º – *Incorpórase como artículo 34 bis del Decreto Nº 2628 del 19 de diciembre de 2002, el siguiente texto: "Aceptación por parte de terceros usuarios de documentos electrónicos firmados digitalmente.*

Los terceros usuarios que sean personas jurídicas que implementen aplicaciones que requieran firma digital, tienen la facultad de definir las características y requerimientos que deben cumplir las Políticas de Certificación, a los efectos de aceptar documentos electrónios firmados digitalmente utilizando certificados digitales amparados por dichas Políticas. Dichas características y requerimientos deben ser manifestados previamente en forma clara y transparente a los titulares de certificados que pretendan operar con ellos".

Art. 5º – *Modifícase el texto del artículo 1º inciso b) del Decreto Nº 2628 del 19 de diciembre de 2002.*

Esta última normativa, que modifica el Decreto 2628/2002 que reglamentó oportunamente la Ley 25506 de firma digital, es de trascendental importancia, ya que de su lectura se desprende, que a fin de lograr la puesta en marcha de la aplicación de la firma digital se modificó lo siguiente:

a) La derogación del artículo 30 del decreto reglamentario, obviándose la necesidad de los seguros vigentes que deben tener quienes soliciten la licencia para actuar como entes licenciantes (autoridades certificantes).

b) Aceptar en sus aplicaciones certificados digitales de certificadores públicos y privados.

c) Conveniencia de la utilización de certificados emitidos por certificadores licenciados públicos en forma gratuita.

d) Se define la figura del *TERCERO USUARIO:* persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta pa-

ra verificar la validez del certificado digital correspondiente. El tercero usuario tiene derecho a aceptar o rechazar documentos electrónicos firmados digitalmente, en certificados cuya política de certificación no reúna las condiciones por él requeridas.

e) Los terceros usuarios que sean personas jurídicas que implementen aplicaciones que requieran firma digital, tienen la facultad de definir las características y requerimientos que deben cumplir las Políticas de Certificación, de forma clara y precisa.

Autoridades certificantes

El certificador licenciado

Análisis de la función notarial y la actividad de los certificadores licenciados

Autoridades certificantes

I. Introducción

Para obtener una firma digital, el solicitante (futuro titular signatario) deberá presentar una solicitud ante un certificador licenciado, quien verificará la veracidad de los datos de la persona del solicitante y, generadas las claves asimétricas que componen a la firma digital, atribuirá a esa firma un certificado digital que permita establecer la correlación entre la clave pública y la privada que la conforman al momento del proceso de verificación de la firma digital.

Conforme al artículo 9º de la ley 25.506, para que una firma digital pueda ser considerada válida es preciso:

a) que esta haya sido creada durante la vigencia del certificado digital del firmante, válidamente expedido por un certificador licenciado; y

b) que pueda ser verificada exitosamente mediante la utilización de los datos contenidos en el certificado digital.

Lo comentado puntualiza la importancia del certificado digital y el certificador licenciado que lo expide, en el sistema de la firma digital implementado por la ley 25.506.

II. Certificados digitales: su contenido y validez

Para la implementación de la firma digital basada en un criptosistema asimétrico, reviste trascendental importancia verificar que la clave pública que la integra esté lógicamente ligada a su clave privada, de modo de asegurar la veracidad de su pertenencia al sujeto firmante del documento electrónico [1].

Técnicamente, el certificado digital [2] es un archivo de aproximadamente 1k de tamaño [3], definido por el estándar internacional ITUT X.509 [4], que asocia una clave pública con la identidad de su propietario.

---

(1) Iturraspe, Urtza; Zaballa, Ivon: *Introducción a los certificados digitales*, en http://revista.robotiker.com/articulos/articulo51/pagina1.jsp Millán, A. J., *La Internet (la WEB). Introducción a la herramienta que condicionará el futuro: 6. Problemas y peligros de la Red*, en http://www.zator.com/Internet/A6_5.htm

(2) Por retiorbi.net: *Transacciones seguras y firma digital,* en http://retiorbi.net/novedades/articulos/junio01.html

(3) Ángel Ángel, José de Jesús, *Firma Digital y Certificados Digitales,* en http://www.htmlweb.net/seguridad/varios/firma_certificados.html

(4) Por PKI Infraestructura de Firma Digital de la República Argentina: *¿Qué contiene un certificado digital?,* en http://www.pki.gov.ar/index.php?option=content&task=view&id=45&Itemid=180

De conformidad con lo establecido por el artículo 14 de la ley 25.506, un certificado digital se considera válido, para nuestro país, cuando ha sido emitido por un certificador licenciado conforme las prescripciones de la ley respondiendo a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación y contiene como mínimo los datos que permiten:

a) identificar indubitablemente a su titular y a su certificador licenciado emisor, así como a la política de certificación [5] bajo la cual fue emitido.

Con anterioridad a la emisión del certificado digital el certificador deberá tomar los recaudos necesarios para garantizar la autenticidad de la identidad del solicitante, verificando su nombre y apellido, nacionalidad, documento, edad, estado de familia y vecindad. Tarea esta que, de no estar a cargo de un "certificador notarial" [6], promovemos sea auxiliada mediante la certificación notarial de la firma en la solicitud del sujeto que pretenda la expedición del certificado a su favor.

b) conocer su período de vigencia o verificar su posible revocación [7]. El artículo 15 de la ley advierte que la fecha de vencimiento del certificado digital "en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió". En consecuencia y por aplicación de lo dispuesto por el artículo 26 del decreto 2628/2002, concluimos que aun cuando no existe un plazo de vigencia fijado legalmente, éste no podría superar al de los 5 años de validez de la licencia concedida al certificador. Sin perjuicio de que, vencido dicho plazo y renovada la licencia, pueda renovarse también el certificado digital.

c) diferenciar claramente la información verificada de la no verificada incluidas en el certificado; y

d) la verificación de la firma digital agregada al documento electrónico, al que el certificado acompaña.

Un certificado no es considerado como válido cuando carece de alguno de los elementos antes mencionados [8], es utilizado con una finalidad diferente para la cual fue emitido, o empleado "en operaciones que superen el valor máximo autorizado cuando corresponda" [9].

Existen diversos tipos de certificados digitales, tales como los de identificación, autorización y tiempo, a la par de categorizarlos de acuerdo con el sujeto destinatario y sus propias funciones como certificados de clase 1, 2, 3, etc. Félix, Walter; Panella, Pablo; Hait, Pablo; Hodari, Graciela; Felicitato, Adrián; Hodak, Bárbara: *Firma y Certificado Digital,* en http://www.hfernandezdelpech.com.ar/Leyes/TRABAJO%20FIRMA%20DIGITAL%20POSTGRADO%20E-BUSINESS.htm

(5) "Conjunto de criterios que indican la aplicabilidad de un certificado a un grupo de usuarios en particular o a un conjunto de aplicaciones con similares requerimientos de seguridad. En inglés *Certification Policy* (CP)". Glosario del decreto 2628/2002.

(6) Ver por Agencia Notarial de Certificación: "Certificados Notariales Personales", en http://www.ancert.com/?do=certificates

(7) Las causales de revocación de un certificado digital están contempladas por la ley 25.506 en el artículo 19, inciso e) y por el artículo 23 del decreto 2628/2002.

(8) Salvo que haya sido emitido por un certificador no licenciado, en cuyo caso el decreto 2628/2002, en el artículo 2, permite que su validez sea acreditada por la persona que pretenda invocarlo.

(9) Art. 23 de la ley 25.506.

III. Certificadores licenciados

El artículo 17 de la ley 25.506 entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados digitales, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

Del texto del artículo podemos concluir que una persona física no podrá ser certificador licenciado. Consideramos que los justificativos de esta limitación se encuentran en que la labor a desempeñar por el certificador licenciado requiere de una infraestructura de recursos financieros, técnicos y humanos que no sería propia de una persona física en singular.

En la actualidad existen numerosos certificadores pero ninguno de ellos "licenciado" por el ente licenciante, bajo los términos de la ley digital y su decreto reglamentario.

Llama la atención la terminología utilizada por el legislador al denominar a los certificadores como "licenciados" en vez de "licenciatarios". Licenciado es toda "persona que se precia de entendida, persona que ha obtenido en la facultad el grado que le habilita para ejercerla o soldado que ha recibido su licencia y, en varios países de América, abogado". Licenciatura es "el grado de licenciado de universidad o estudios necesarios para obtener este grado". A su vez, por licencia se significa a "la facultad o permiso para hacer algo". Por ello, cabría referirse a los certificadores como licenciatarios, es decir como usuarios de la licencia conferida por el ente licenciante.

Conforme el artículo 20 de la ley, para obtener una licencia, el certificador deberá tramitar la solicitud respectiva ante el ente licenciante, el que la otorgará previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones, resultando estas licencias intransferibles. Ello, además de cumplir con lo prescripto por el capítulo VIII del decreto 2028/2002.

Estos certificadores deben constituir domicilio en la República Argentina y obtener la aprobación del ente licenciante en cuanto al manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar en sus funciones. Tienen a su cargo la emisión, preservación, revocación y publicidad de los certificados digitales, así como la identificación de sus solicitantes y la prestación de servicios accesorios con relación a las firmas digitales, todo ello en el cumplimiento de las funciones y obligaciones impuestas respectivamente por los artículos 19 y 21 de la ley 25.506 y el artículo 34 del decreto 2628/02.

Resulta imperativa la confidencialidad de toda información que no figure en el certificado digital, por lo que se le exige al certificador que, bajo cualquier circunstancia, se abstenga de acceder, exigir, por cualquier otro medio tomar conocimiento o divulgar los datos de creación de la firma digital de los titulares de certificados digitales por él emitidos.

IV. Recursos de los certificadores licenciados

1. De acuerdo con el artículo 32 del decreto 2628/02, para el desarrollo adecuado de las actividades de certificación, el certificador deberá acreditar

que cuenta con un equipo de profesionales, infraestructura física, tecnológica y recursos financieros, así como también procedimientos y sistemas de seguridad que permitan:

a) Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia, así como garantizar la confiabilidad de los sistemas para la expedición y administración de certificados digitales válidos, de acuerdo con los estándares aprobados por la autoridad de aplicación y conforme la ley 25.506.

b) Cumplir con lo previsto en sus políticas y procedimientos de certificación.

c) Proteger el manejo de la clave privada de la entidad mediante un procedimiento de seguridad que exija la participación de más de una persona, e impida su acceso a personal no autorizado.

d) Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.

e) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.

f) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.

2. Tercerización de la infraestructura tecnológica

El certificador licenciado, para cumplir con las funciones a su cargo, requiere de una inversión cuantiosa en el desarrollo y actualización de la tecnología necesaria para procesar la solicitud, emisión y verificación de un certificado digital; todo ello bajo una infraestructura de máximo nivel de seguridad que garantice un porcentual mínimo de vulnerabilidad de los sistemas utilizados [10].

Por ello, el artículo 33 del decreto 2628/02 ha previsto que los certificadores licenciados puedan celebrar contratos con proveedores de servicios de infraestructura a fin de utilizar los servicios de infraestructura tecnológicos desarrollados por ellas.

En este supuesto de tercerización de la infraestructura tecnológica para llevar a cabo sus funciones, el certificador licenciado deberá contemplar dentro de su Plan de Contingencia los procedimientos a seguir en caso de interrupción de estos servicios, de modo tal que le permita continuar con prestaciones sin ningún perjuicio para los titulares de los certificados digitales por él emitidos.

El certificador licenciado o en proceso de licenciamiento deberá facilitar al Ente Licenciante toda aquella información obrante en los contratos celebrados con la empresa proveedora que esté vinculada a la prestación de servicios de certificación y a la implementación del Plan de Cese de actividades y el Plan de Contingencia.

Los contratos entre el certificador licenciado y los proveedores de servicios o infraestructura deberán garantizar la ejecución de los procedimientos

(10) Existen numerosas empresas en el mercado cuyo objetivo comercial es la venta de esta tecnología y la asistencia tecnológica soporte técnico durante su utilización. Ej: VeriSign.

contemplados en el Plan de Cese de actividades aprobado por el Ente Licenciante.

3. Responsabilidad del certificador licenciado por la tercerización de la infraestructura tecnológica

Cualquier daño o perjuicio ocasionado al titular de un certificado digital expedido por el certificador licenciado o a un tercero, derivado de la aplicación de una firma digital basada en una infraestructura tecnológica deficiente provocadora del daño, queda bajo la responsabilidad primaria del certificador licenciado; sin perjuicio de que éste pueda accionar contra la empresa proveedora de la tecnología por repetición y la responsabilidad solidaria que pueda invocar el perjudicado contra ambos.

V. Autoridades de Registro

1. Concepto. Funciones

Los certificadores licenciados podrán delegar en autoridades de registro las funciones de validación de identidad y de otros datos de los suscriptores de certificados y el registro de las presentaciones y trámites que les sean formulados.

La autoridad de registro se presenta como un auxiliar para el certificador licenciado en cumplimiento de sus funciones. Su presencia no es obligatoria, por lo que habrá certificadores licenciados que deleguen parte de sus funciones en autoridades de registro y otros que no lo hagan.

A su vez, la autoridad de registro puede estar conformada como una única unidad o varias unidades dependientes jerárquicamente entre sí; en este último caso, siempre que medie la aprobación del certificador licenciado.

Es función propia de las autoridades de registro verificar la identidad del solicitante de un certificado digital, recepcionar la solicitud y, una vez aprobada, remitirla al certificador licenciado del que depende, para que se expida sobre la emisión del certificado digital solicitado.

Igual tarea le compete ante el pedido de revocación de un certificado digital expedido por el certificador licenciado con el que se encuentra vinculada. Recibirá la solicitud de revocación y, previa verificación de la identidad del solicitante, la remitirá al certificador licenciado para que él proceda a su revocación.

Todas estas obligaciones debe desempeñarlas en cumplimiento de las normas y recaudos establecidos para la protección de datos personales y las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del certificador licenciado con el que se encuentre vinculada.

A nuestro juicio, el autor equivoca los conceptos participando de la creencia de la falta de utilidad de un mecanismo de autenticación que simultáneamente pone en evidencia como imprescindible, apelando al sentido común por él proclamado.

2. Responsabilidad del certificador licenciado repecto de la autoridad de registro

El certificador licenciado es responsable primario por los daños y perjuicios que el accionar u omisión de la autoridad de registro ocasionare, sin perjuicio del derecho del certificador de reclamar a la autoridad de registro por repetición y la acción que entablare el titular del certificado o el tercero contra ambos, a mérito de la responsabilidad solidaria que competa por el daño causado.

VI. Certificadores licenciados y la certificación notarial de la Firma Digital

No debe confundirse la función identificadora del solicitante de una firma digital, cumplida por el certificador licenciado o las autoridades de registro, con la certificación notarial de la firma digital [11].

El certificador licenciado y/ o autoridad de registro sólo se encargará de individualizar al firmante antes de emitir el certificado digital [12] y garantizar su vigencia una vez emitido, siendo el notario como profesional de derecho depositario de la fe pública el único que podrá certificar la identidad del firmante en el acto de suscribir el documento electrónico.

En este supuesto y en caso de conflicto, la certificación notarial dará fe: a) de que la firma digital certificada ha sido aplicada mediante el uso del certificado digital declarado; y b) de la identidad del sujeto firmante. Lo que es equivalente a afirmar que una firma digital, certificada notarialmente, no será pasible de repudio sino mediando juicio de redargución de falsedad [13].

La firma digital es sólo una nueva forma de suscribir documentos, que no posee por el momento mayor credibilidad que la de la firma ológrafa privada. Por ello no invalida al sistema notarial imperante, requiriéndose para su certificación la comparecencia presencial del signatario y el estampado de su firma ante el notario certificante [14].

Está claro que admitir este tipo de certificaciones implicaría modificar de manera sustancial al Reglamento de Certificación de Firmas e Impresiones Digitales vigente [15].

---

(11) Situación reconocida en:
http://www.pedrodelpiero.com.ar/common/files/discurso_sancion_firma_digital.doc

(12) Esta función, como quedó dicho, proponemos sea auxiliada con la intervención notarial dando fe de conocimiento del solicitante.

(13) En una posición contraria y considerándolo innecesario, ver: González-Bueno, Carlos, *La firma electrónica ante el notario,* en http://www.belt.es/expertos/experto.asp?id=1714.

(14) Devoto, Mauricio, *Responding to the legal obstacles to electronic commerce in Latin America,* en http://www.natlaw.com/ecommerce/presentations/devoto.doc

(15) Sobre un procedimiento sugerido para la certificación notarial de una firma digital, ver: Pérez Clouet, María José, "El notario y la contratación electrónica: documento electrónico y firma digital", *Revista Notarial* nº 948, pp. 352 y ss.

VII. El Consejo Federal del Notariado Argentino como certificador licenciado y los colegios notariales y sus notarios como autoridades de registro

La infraestructura de la firma digital se construye sobre la base de la confianza depositada en los certificadores licenciados, encargados de la emisión y administración de los certificados digitales.

Estos recursos podrían ser tercerizados en los términos y con el régimen de responsabilidad explicados en los apartados precedentes.

Entendemos que el notariado argentino se encuentra en condiciones de constituirse en certificador licenciado de los certificados digitales que sean solicitados por cualquier miembro integrante de la sociedad, por ser una institución de reconocido prestigio profesional que goza de la confianza colectiva y ejercer su actividad habitual de manera compatible con las funciones propias de este tipo de certificadores.

Bajo este contexto, concebimos al Consejo Federal del Notariado Argentino como certificador licenciado; el que debería conformarse con los recursos humanos y tecnológicos necesarios para generar, renovar, suspender, revocar y preservar a los certificados digitales que serían por él emitidos.

Los Colegios de Escribanos de nuestro país, mediante los notarios que correspondan a cada demarcación, se sumarían a la propuesta como colaboradores (autoridades de registro o registradoras) constituyendo el vínculo directo entre el Consejo Federal como certificador licenciado y los solicitantes de los certificados digitales. Ellos recibirían y remitirían las solicitudes de expedición de los certificados al Consejo Federal, validarían la autenticidad de la identidad de los solicitantes, conservarían su documentación respaldatoria, y procesarían las denuncias de revocación.

De esta manera, a través de los notarios y las delegaciones notariales de cada uno de los Colegios notariales, se generaría una red de servicio que abarcaría la totalidad del territorio nacional, facilitando el acceso de la población a la infraestructura de la firma digital.

Conclusiones

1. La firma digital es la representación binaria personal y distintiva del sujeto firmante, capaz de generar un vínculo de imputación en cuanto al contenido del instrumento en el cual se aplique, como forma de expresión de su voluntad.

2. Una firma digital se considerará válida cuando sea aplicada durante el período de validez del certificado digital que le corresponda, previamente emitido por un certificador que haya obtenido su licencia del ente licenciante, en los términos de la ley 25.506.

3. Aun cuando no existe un plazo de vigencia fijado legalmente para el certificado digital, éste no puede superar al de los 5 años de validez de la licencia concedida al certificador.

4. Las personas físicas no podrán ser certificadores licenciados.

5. Es incorrecta la terminología utilizada por la ley al referirse al certifica-

dor licenciado pues debió individualizarlo como certificador licenciatario de la licencia concedida por el ente licenciante.

6 La autoridad de registro se presenta como un auxiliar para el certificador licenciado en cumplimiento de sus funciones, cuya existencia no es obligatoria.

7. Con anterioridad a la emisión del certificado digital, el certificador licenciado o autoridad de registro deberá tomar los recaudos necesarios para garantizar la autenticidad de la identidad del solicitante, verificando su nombre y apellido, nacionalidad, documento, edad, estado de familia y vecindad; tarea esta que, de no estar a cargo de un "certificador notarial", promovemos sea auxiliada mediante la certificación notarial de la firma en la solicitud del sujeto que pretenda la expedición del certificado a su favor.

8. La entidad certificadora o autoridad de registro sólo se encarga de individualizar al firmante antes de emitir el certificado digital y garantizar su vigencia una vez emitido, siendo el notario como profesional de derecho depositario de la fe pública el único que puede certificar la identidad del firmante en el acto de suscribir el documento electrónico.

9. Una firma digital certificada notarialmente no será pasible de repudio sino mediando juicio de redargución de falsedad.

10. Resulta conveniente que el Consejo Federal del Notariado sea habilitado como certificador licenciado de firmas digitales de cualquiera de los miembros de la sociedad, con el auxilio de los Colegios de Escribanos y Notarios en particular, como autoridades de registro.

11. El Consejo Federal del Notariado Argentino, para cumplir con su tarea de certificador licenciado, podrá tercerizar el servicio de infraestructura tecnológica.

Breve análisis de la función notarial y la actividad de los certificadores licenciados de la ley 25.506

De la lectura de las leyes notariales de nuestro país y la actividad que revestirán en un futuro mediato los certificadores licenciados, antes definidos y sin perjuicio de las grandes diferencias entre ambos sujetos de derecho, corresponde apuntar algunos aspectos que, a nuestro modo de ver, deben ser tenidos en cuenta sólo en cuanto la actividad pueda ser coincidente o, aunque sea, semejante.

a) Valor de las firmas

Cuando el escribano certifica que la firma ha sido estampada por ante él hace plena fe de ello y corresponde una acción civil o penal de redargución de falsedad a quien intente probar lo contrario, obviamente estando a cargo de quien lo alega la tarea de desvirtuar tal presunción y con traslado al notario que ha certificado la firma.

Por su parte, los *certificadores licenciados* certifican que la firma pertenece a su titular con un valor probatorio relativo y que admitiría una mera comprobación de hecho en contrario pero la ley le otorga una presunción a su favor (art. 7) poniendo la carga de la prueba a quien le niegue autenticidad, cosa que la hace diferir enormemente de los instrumentos privados en general (obviamente, sin certificación de firma).

Esto significa que las firmas digitales tienen un valor probatorio mayor que las puestas en el soporte papel y están más cerca en este aspecto a las firmas certificadas por notario.

b) Actos jurídicos posibles

Podría argumentarse, para marcar diferencias, que existen en la actualidad actos jurídicos excluidos de la competencia de los certificadores licenciados, como las disposiciones por causa de muerte; los actos jurídicos del derecho de familia; los actos personalísimos en general; los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes (art. 4º ley 25.506).

Sin embargo, algunos estudiosos del tema estiman que esta exclusión es meramente temporal y de ninguna manera subsistirá cuando la utilización de este medio sea generalizada y, en su caso, probados que sean su funcionamiento y fidelidad.

c) Delegados del Estado

Los escribanos públicos, para acceder a la función, son designados por el Estado (en la Ciudad de Buenos Aires y otras jurisdicciones del país, previamente deberán aprobar el examen de oposición y antecedentes, tanto para obtener la titularidad de un registro y/ o acceder a una adscripción, conforme

al puntaje obtenido). Esta investidura hará que ejerza su actividad fedante como un delegado del Estado, depositario de la fe pública.

El sistema de firma digital, en principio, también deja recaer sobre el Estado la potestad certificante o de expedición de certificados; sin embargo, prevé además la posibilidad de licenciar en personas jurídicas o físicas el ejercicio de estas potestades.

d) Archivos

Los notarios llevan un registro especial para el requerimiento de certificación de firmas, protocolos y el índice anual que expresara de cada instrumento, nombre de los otorgantes, fecha de otorgamiento, naturaleza del acto y primer folio de la escritura. Su función de archivo de documentos es reconocida y obligatoria por ley; asimismo, está obligado a entregar al Estado los protocolos de los últimos años, siendo distinto en cada jurisdicción.

A los certificadores licenciados se les ha encomendado mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento y de sus correspondientes solicitudes de emisión, debiendo, además, mantener la documentación respaldatoria de los certificados digitales emitidos por 10 (diez) años a partir de su fecha de vencimiento o revocación y deben llevar un registro de las transacciones realizadas a fin de identificar al autor y el momento de cada una de las operaciones. Por último, deben enviar periódicamente al Ente Administrador informes de estado de operaciones con carácter de declaración jurada.

En este aspecto, las funciones de "archiveros" y "registradores" no resultan muy distintas en lo que hace a la faz interna y respecto de la información que deben brindar al Estado.

e) Seguridad y confidencialidad

La profesión de escribano implica una confianza por parte de los requirentes, lo que hace que en muchos casos se maneje cantidad de información personal, familiar y patrimonial de los otorgantes, por lo que la ley establece la necesidad de mantener el secreto profesional sobre todo acto en que intervenga en el ejercicio de su función.

En los sujetos de la firma digital que venimos analizando es necesario, según la ley, garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados y proteger a todos los sistemas utilizados en la función de certificación. Además, deben abstenerse de generar, exigir o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por ellos emitidos e impedir su divulgación. Es por ello que, al igual que los escribanos, deben mantener la confidencialidad de toda información que no figure en el certificado digital.

f) Certificación

Conforme la definición expuesta, ambos sujetos dan testimonio o docu-

mento justificativo de la verdad de algún escrito y dan fe de algo que les consta, por lo que sin dudas ambos certifican.

g) Responsabilidad

Se ha apuntado que los escribanos responden con su patrimonio por los daños causados en virtud de su actuación.

Por su parte, el certificador que emita un certificado digital o lo reconozca es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles (art. 38 ley 25.506).

h) Sanciones

Ambos sujetos son pasibles de sanciones por el incumplimiento de las obligaciones establecidas en la ley.

i) Repudio de contenido

Los escribanos, como operadores de derecho, están obligados a no otorgar o certificar actos contrarios al derecho, la moral y las buenas costumbres. Sin embargo y pese a que es el Estado quien les delega facultades certificantes, los certificadores licenciados no están obligados a repudiar u observar los contenidos de los documentos, así por ejemplo, podría pasar por sus registros un documento firmado digitalmente sobre trata de blancas o prostitución infantil, sin que ello pudiera ser observado por lo menos en ese ámbito. Al provenir sus facultades del Estado, esto resulta por lo menos descabellado.

j) Fecha cierta

La certificación de la firma ológrafa dota de fecha cierta al instrumento sujeto a certificación pues un notario está dando fe de que las firmas son de puño y letra del requirente y de que han sido estampadas en el día indicado.

Paralelamente, las autoridades certificantes pueden ofrecer servicios de fechado de un documento, lo que le otorga fecha cierta.

k) Instrumentos públicos

Entienden algunos autores que los escribanos están facultados a confeccionar instrumentos públicos, es decir, escrituras públicas y demás actos autorizados en la ley de cada demarcación, todo ello bajo las normas que surgen del Código Civil. Si una disposición legal facultara a un escribano a otorgar documentos electrónicos y conferirles autenticidad, estos no participarían de idéntica naturaleza. En última instancia y dada la carencia de firma (tradicional), aunque sea podría justificarse la presunción legal de los arts. 7 y 8 de la ley 25.506.

Pese a las semejanzas apuntadas y a la función que realizarán en el futuro los certificadores licenciados, estos no necesitan de mayores requisitos para

constituirse en tales. **Diferencia profunda con los escribanos, que encuentran la dificultad de reunir cantidad de requisitos, sortear inhabilidades y luego incompatibilidades.**

Las diversas exigencias establecidas a los escribanos (ser ciudadano argentino, tener residencia inmediata, mayoría de edad, título; acreditar buena conducta, matriculación etc.) tienen su justificación por cuanto realizan una importante función social ya que son asesores, fedantes, archivos de datos y manejan cantidad de información, por lo que merecen una formación, una investidura y un control determinados. Ahora bien, dadas las coincidencias apuntadas y atento al futuro de la firma digital, cabe preguntarse: **¿Cuál es el motivo por el cual no se han establecido mayores requisitos, inhabilidades e incompatibilidades a los certificadores privados en la ley 25.506?**

¿Estamos en presencia de una nueva actividad certificante? ¿A ser una actividad privada de libre competencia? Unas de las más importantes empresas dedicadas a la certificación cuenta entre su equipo de trabajo, sin desmerecer su actividad ni sus antecedentes, con docentes, licenciados en administración de empresas, contadores, licenciados en matemáticas, licenciados en computación, sin otro requisito que la aceptación según el criterio de quien esté al frente de la sociedad. Estas empresas y sus integrantes pueden ser los encargados de brindar la confianza necesaria y garantizar los intercambios que se realizan sobre redes públicas, realizando la autenticación e identificación de las personas involucradas en las transacciones, garantizando "integridad" de la información y confidencialidad de la información.

Visto desde esta óptica, su actividad no es suficiente para suplir la fe pública delegada por el Estado a los escribanos; las tareas y funciones parecen similares, pero son totalmente distintas. Debe tenerse en cuenta que los certificados digitales que expiden estas "empresas" y/ o personas jurídicas solamente afirmarán en la consulta que realice un receptor de documento firmado digitalmente que: "*el certificado de firma digital de… se encuentra en período de validez desde el… hasta el… no ha sido revocado y se extendió a… titular del documento de identidad… quien actúa… siendo la política de certificación de…*".

Basta sólo recordar lo que se apuntó al principio de este trabajo: "La verdadera función de la firma es, en efecto, la función declarativa, que es la que exige esa actuación personal del signante. *Una firma declara muchas cosas: declara que aquello es un documento, y no un proyecto o borrador, puesto que no hay documento sin autor; declara, al ser suscripción, que el documento está terminado, declara que el firmante asume como propio el documento, y lo aprueba y confirma, en el concepto, y en la medida que el mismo instrumento establece. Pero la firma no se limita al documento, pues lo que principalmente se firma es su contenido, las manifestaciones o declaraciones que el firmante efectúa mediante el documento y, por lo tanto, en los documentos negociales, su declaración de voluntad*".

Desde otro punto de vista, otra problemática que se presenta es que los instrumentos privados en general carecen de valor probatorio mientras la firma que lo suscribe no haya sido reconocida por el interesado o declarada debida-

mente reconocida por juez competente. Este principio también es aplicable respecto de la modificación de los instrumentos.

Sin embargo, el documento firmado digitalmente trae aparejada una presunción legal de autoría e inalterabilidad que nos hace pensar sobre la necesidad de establecer mayores exigencias a los certificadores licenciados, para aquellos que quieren conferir a su actuación más certeza de la única que pueden dar conforme a la ley.

Nos resulta algo incómodo e incomprensible, a quienes aún creemos en la secular institución del Notariado, el hecho de que similares funciones sean ejercidas hoy por sociedades anónimas, anonimato que se extiende a sus antecedentes, integrantes, capital, origen, etcétera.

Estos temas requieren de pronta atención ya que no falta mucho para que la firma digital llegue a los hogares de todos los argentinos.

La certificación, la presunción de autoría e inalterabilidad, inversión de la carga de la prueba, la posible futura ejecutividad de un instrumento digital queda hoy en manos de corporaciones, a las que no se les exige mayores requisitos.

De hacer caso omiso a esta tarea no resultará descabellado, y siempre y cuando se mantenga la actual legislación, un planteo de inconstitucionalidad en los términos del art. 16 de nuestra Constitución nacional por parte de algún notario.

Ref. Artículo publicado en Suplemento de Derecho Administrativo. *El Dial Express Doctrina Internet.*

Albrematica S. A. "Internet, firma digital y la certificación". Por Juan Pablo Alborno Kokot Comentarios: Esc. Ana María Kemper.

Jurisprudencia argentina sobre documento electrónico

- Consideraciones previas
- Caso
- Prueba en el derecho informático
- Su apreciación en los estrados judiciales

Jurisprudencia argentina sobre documento electrónico

Previo al tratamiento de los casos jurisprudenciales, es importante tener en cuenta las definiciones que a continuación se detallan:

Se denomina documento la entidad jurídica que constituye un instrumento; por otra parte, el término "electrónico" o "informático" no avala la noción que se intenta transmitir del modo en que lo hace el término "digital".

El término "electrónico" se refiere al dispositivo en el que se almacena el instrumento; en cambio, el vocablo "digital" tiene una connotación diferente que implica ausencia de tangibilidad.[1]

En el plano procesal, o sea en la prueba como medio para demostrar la veracidad de lo que se pretende o defiende, la dificultad se da en la aceptación del documento o instrumento informático como medio de prueba en juicio.

Los distintos fueros se han expedido de variada manera al respecto, sin perjuicio de que se trata de un hecho nuevo, de estos tiempos, y hace falta la adaptación que brinde la seguridad jurídica que un pronunciamiento judicial debe brindar.

Ya en 1990 la Cámara Nacional de Apelaciones en lo Comercial se expidió sobre el valor. El Tribunal sostuvo al pronunciarse sobre el valor probatorio de una pericia efectuada sobre información contenida en una computadora [2], que la negativa a admitir liquidaciones efectuadas sobre registros regulares llevados por computación no significaba impugnar los montos que aparecían en el estado de las cuentas.

El plano sustancial del problema que se suscita por la voluntad exteriorizada informáticamente nos sumerge en el tema de la forma de los actos jurídicos, los cuales califica el codificador en forma liberal, permitiendo a las partes elegir la que consideren más conveniente y que haga a sus necesidades e intereses, ya sea en práctica o en tiempo.

En análisis minucioso, debemos concluir que en cuanto los requisitos formales exigidos sean menores, más probable es la utilización de medios informáticos en la celebración de los distintos actos.

Un criterio de avanzada permitirá decir que Vélez Sarsfield se inspiró en la redacción del art. 973, de manera tal que seguirán usándose las formalidades

(1) Sarra, Andrea, *Comercio electrónico y Derecho,* Ed. Astrea, p. 346.
(2) CNCom., Sala D, 21990 *ED* 142-185.

establecidas ya que estas vienen utilizándose desde hace más de 2000 años, dado que lo que ha ido avanzando y cambiando es la simbología, acorde con el avance de las tecnologías que permiten cambiar de la palabra escrita sobre papel a la expresión de la voluntad por medios digitales.

Como coordinadora, he tenido en cuenta en este estudio de investigación y desarrollo del documento electrónico en la República Argentina, qué sucede en los estrados judiciales de nuestro país, cuando llegan a ellos causas vinculadas con documentos soportados en forma electrónica y/ o digital. Se han tenido en cuenta casuísticas sucedidas en los tribunales de la Ciudad de Buenos Aires.

En primer lugar, y siguiendo un orden cronológico, es de suma importancia la resolución del fallo de la Cámara Nacional de Apelaciones en lo Criminal y Correccional, que ***equiparó el correo electrónico a la correspondencia epistolar y le brindó similar protección jurídica*** [3]. En los autos "Martolio c/ Lanata" se sostuvo que: *"el correo electrónico posee características de protección de la privacidad más acentuadas que la inveterada vía postal a la que estábamos acostumbrados, ya que para su funcionamiento se requiere un prestador del servicio, el nombre del usuario y un código de acceso que impide a terceros extraños la intromisión en los datos que a través del mismo puedan emitirse o archivarse. Sentadas estas bases preliminares, nada se opone para definir al medio de comunicaciones electrónico como un verdadero correo en versión actualizada".*

Posteriormente, la Cámara Nacional de Apelaciones en lo Civil, Sala I, en su resolución del 11 de agosto de 2005, no validó como "prueba" ***los mensajes de correo electrónico de e-mails y faxes*** mantenidos entre las partes, por los cuales se pretendía atribuir la existencia y validez de un contrato de mutuo. Entendió el tribunal que al no haberse configurado la relación contractual, no podía ejecutarse la obligación que eventualmente se hubiera convenido entre las partes, por este medio.

Caso Tribunal

Cámara Nacional de Apelaciones en lo Civil, Sala I.

FECHA: 11/08/2005.

PARTES: Leone, Jorge N. c/ Maquieira, Jorge S.

Publicado en La Ley 14/12/2005.

El actor demandó con fundamento en un mutuo celebrado con el demandado con quien tenía una relación de amistad, dicho contrato no fue instrumentado por escrito, por lo que acompañó a los efectos probatorios distintos *e-mails* y faxes que intercambiaron.

El juez rechazó la demanda luego de ponderar que la prueba presentada no había logrado acreditar la existencia del contrato. La Cámara confirmó la sentencia apelada.

---

(3) *La Ley,* 1999C, 458.

Hechos

1. No puede tenerse por acreditada la existencia del contrato de mutuo que se pretende ejecutar, ya que si bien se acompañaron las copias de los *e-mails* que intercambiaron las partes, no existe prueba sobre la autenticidad de los correos electrónicos atribuidos al demandado y enviados a través de la casilla que se le adjudica, máxime cuando el actor tenía a su alcance otros medios para acreditar su autenticidad, como ser, el secuestro del disco rígido con carácter cautelar o el ofrecimiento de perito especializado en la materia.

2. La ausencia del requisito de firma que regula el art. 1012 del Cód. Civil para la configuración de un instrumento privado, no impide que pueda considerarse al *e-mail* en los términos del art. 1190, inc. 2 como "instrumento particular no firmado" a los fines de acreditar la existencia de un contrato o bien como "principio de prueba por escrito" en los términos del art. 1191 del citado Código.

La Ley

El art. 2246 del Código Civil dispone que "el mutuo puede ser contratado verbalmente; pero no podrá probarse sino por instrumento público o instrumento privado de fecha cierta, si el empréstito pasa del valor de diez mil pesos" (texto según ley 17.940).

Aunque es claro que esta limitación sólo se aplica a las relaciones con terceros, pues entre las partes rigen los principios generales de los arts. 1191 y 1192 del Código Civil.

Desde esta óptica entraré a analizar la prueba traída por el actor, sobre a quién pesa la carga de acreditar la existencia del contrato que invoca como celebrado verbalmente con el demandado (art. 377 del Código Procesal).

Cabe destacar la fragilidad de la prueba aportada, pues si bien es cierto que a fs. 7/13 se acompañan las copias de los *e-mails* que se dicen intercambiados por las partes, no existe prueba sobre la autenticidad de los correos electrónicos atribuidos a Maquieira, enviados a través de la casilla que se le adjudica.

No se trata de restar valor probatorio a este medio de prueba sino de señalar su insuficiencia en los términos pretendidos.

Tengo en cuenta para esto que estamos frente a una figura novedosa, cuya equiparación con los instrumentos privados que regula el art. 1012 del Código Civil se encuentra obstaculizada por la ausencia de firma.

De todos modos, la ausencia de este requisito, que la ley estipula esencial para la configuración de un instrumento privado, no impide que pueda considerarse al *e-mail* en los términos del art. 1190, inc. 2, como "instrumento particular no firmado" a los fines de acreditar la existencia de un contrato o bien como "principio de prueba por escrito" en los términos del art. 1191 Código Civil.

En tal sentido se ha dicho que "en nuestro derecho, para poder probar la existencia de un contrato, si la ley requiere una forma determinada para su celebración, no podremos probarlo si no estuviere hecho en la forma prescripta, a excepción de que existirá principio de prueba por escrito en los contratos

que pueden hacerse por instrumento privado (art. 1191 C.C), esto es, por instrumentos particulares no firmados, por confesión de parte –judicial y extrajudicial–, por juramento judicial, por presunciones legales o judiciales y por testigos" (Luis Mauricio Gaibrois, "Un aporte para el estudio del valor probatorio del documento electrónico", *JA* 1993II956).

Agrega el autor citado que "el documento electrónico […] puede presentarse en el juicio a los efectos de probar un contrato, siempre que emane del adversario y haga verosímil el hecho litigioso; todo ello, claro está, cuando el cúmulo de las restantes pruebas, examinadas todas a la luz de la sana crítica procesal, determine que el juez le acuerde autenticidad".

Guillermo A. Borda, *Contratos*, t. II, 2090 y sus citas.

Bueres, Alberto J. y Highton, Elena I., t. 4E. "Análisis del art. 2246", pp. 362 y ss. en *Código Civil y normas complementarias. Análisis doctrinario y jurisprudencial.*

Jurisprudencia. Prueba en el derecho informático: su apreciación en los estrados judiciales

Nota al fallo relacionado del Dr. Juan Martín Alterini, artículo "Nuevamente sobre la Prueba en el Derecho Informático", publicado en Revista La Ley. (Argentina)

El fallo que antecede ha dado una serie de definiciones y tratamiento jurisprudencial sobre el valor probatorio en el derecho informático, lo que ha sido receptado en forma muy elocuente por el Dr. Juan Martín Alterini, quien en su nota a fallo publicada en *La Ley* el 14 de diciembre de 2005 trata el tema y sostiene: *"la falta de sincronismo entre tecnología y Derecho presenta problemas más imaginarios que reales; nuestro sistema jurídico es capaz de salir airoso de los embates y desarrollos a que le someten los ordenadores y Ciberespacio"* [4].

La tarea interpretativa a cargo del juez puede ser llevada, cada vez con mayor esfuerzo, a buen puerto. En ese entendimiento recobran plena vigencia las palabras de la Dra. Graciela Messina de Estrella Gutiérrez, quien en un meduloso trabajo de investigación sostuvo que: *"Actualmente nadie duda de que el mundo ha ingresado en una era distinta; la tecnología o sociedad de la información. La nueva riqueza de las naciones está constituida por el Know how o recurso estratégico de la información; ahora se produce información en masa del mismo modo que los países en masa"* [5]. De manera tal que el cúmulo de infor-

(4) Nicoll, Christopher, citado en Paz Cándido - Ares Rodríguez - Bermejo Gutiérrez, Nuria - Saen Lacave, M. Isabel, "La formación electrónica del contrato: Nada nuevo bajo el sol", *Derecho sobre Internet,* Banco Santander Central Hispano - Asesoría Jurídica del Negocio, Madrid, p. 2.

(5) *La responsabilidad civil en la era tecnológica*, Abeledo Perrot, Buenos Aires, 1997, pp. 75/76.

mación, que hoy constituye fuente de riqueza, requiere de un marco jurídico que la contenga y establezca las reglas del juego [6].

Agrega Alterini que *"como en tantas otras, las clasificaciones del derecho y los términos con que habitualmente nos entendemos, evidencian su imperfección. En verdad, no habría por qué llamar procesal al derecho de defenderse y material o sustancial al derecho defendido. En cierto modo, el derecho de defenderse es un derecho sustancial, y en muchos aspectos lo es más que el derecho debatido en juicio. Pero es su ejercicio en un proceso lo que hace que en esta materia, como en otras, utilicemos la tan artificial distinción del derecho procesal y del derecho material"* [7]. En el Derecho de daños, el Derecho de fondo y el de forma se unen a un punto tal que se torna inescindible del pensamiento técnico el uno del otro [8].

El comentario que realiza el Dr. Alterini del fallo antes descripto sostiene que aporta conceptos a la ciencia de fondo, y en cuanto a la de forma, vemos que se deberá intentar continuar la construcción de una novedosa disciplina.

De la lectura de la sentencia surge con evidencia que el problema a elucidar por el Tribunal de alzada radicó en la ausencia de prueba del referido contrato y, en especial, que la que se aportó al expediente no resultó suficiente como para esclarecer la controversia.

Por un lado, la existencia misma del contrato; por el otro, si con los instrumentos electrónicos *–e-mails–* se pueden tener por probadas las afirmaciones del actor en su escrito de postulación y, consecuentemente, revocar la sentencia de la primera instancia que desestimó el planteo.

Así las cosas, luego de un profundo análisis de la temática involucrada, y en la interpretación del Tribunal, se homologó la decisión apelada.

Sostuvo la alzada: *"Conviene detener el análisis en la prueba referida a la existencia misma del contrato que se invoca, pues ésta y no otra es la cuestión controvertida en el caso, concluyendo que la prueba aportada no resultó suficiente como para que el planteo progresara"*.

Resulta necesario remarcar otro pasaje de la resolución como para delimitar, en lo que hace a este trabajo, el sentido que se busca proponer: así, se sostuvo que *"estamos frente a una figura novedosa, cuya equiparación con los instrumentos privados que regula el art. 1012 del Cód. Civil se encuentra obstaculizada por la*

(6) Nótese que cuando la doctora Messina de Estrella Gutiérrez alude a la sociedad de la información está significando lo que en las normas de la Comunidad Europea es la Internet. Ello, en palabras de Canavillas Mugica, obedece a la dificultísima caracterización de un sistema de comunicación que evoluciona día tras día y cuyo nombre, sin dudas, puede modificarse en función de tal avance. De ese modo, todo lo que se regule con denominación "Internet" perdería actualidad con el simple y previsible cambio de la técnica que le permite operar y consecuentemente, su denominación.

(7) Couture, Eduardo J., *Fundamentos del Derecho Procesal Civil*, 3ª edición, Depalma, Buenos Aires, 1997, p. 96.

(8) Como alguna vez lo señalara (*La responsabilidad del abogado en el marco de la teoría de las obligaciones de resultado atenuadas,* RCyS, 2001418; *www.jmalterini.com/jmalterini.html*). En la responsabilidad civil, el Derecho Procesal es al Derecho de fondo lo que un Reglamento a un deporte.

ausencia de firma. De todos modos, la ausencia de este requisito, que la ley estipula esencial para la configuración de un instrumento privado, no impide que pueda considerarse al e-mail *en los términos del art. 1190 inc. 2) como 'instrumento particular no firmado' a los fines de acreditar la existencia de un contrato o bien como 'principio de prueba por escrito' en los términos del art. 1191 Cód. Civil".*

Las conclusiones del Tribunal

En la difícil tarea de condensar un nutrido precedente y efectuar las conclusiones que merece, tomando como punto de partida los tópicos antes señalados:

a) En primer lugar, aparece la prueba del contrato de mutuo que se dice haber celebrado, para continuar –en lo que surge del texto de la sentencia– con la prueba de éste y de las afirmaciones propuestas por el actor.

No hay discusión acerca de que el correo electrónico, tal como lo dijo el Tribunal, constituye un tipo de instrumento que se denomina instrumento particular no firmado [9].

Al ser ello así, y en lo que se vincula con su régimen probatorio, los instrumentos particulares no firmados pueden ser reconocidos judicial o extrajudicialmente. De ello se sigue que, para lograr su prueba, también están en juego las presunciones que se forman con un cúmulo de indicios y la prueba testimonial que, a los efectos de la prueba de los instrumentos particulares en el ordenamiento argentino vigente, carece de sentido, ya que tanto el Código Civil como el de Comercio establecen límites para que sea procedente dicho medio de prueba; límites que hacen que la mayoría de los contratos por su cuantía no puedan probarse por testigos [10].

De manera tal que si entendemos por documento *a aquello que formado en presencia de un hecho, su destino es fijar de modo permanente su representación verbal o figurativa, de modo que pueda hacerlo conocer a distancia de tiempo* [11], adoptaremos una concepción amplia, sin duda, que permite considerar a las Pirámides egipcias como documento, ya que *predican algo, representándolo verbal o figurativamente y hacen conocer visiones de la realidad que los cobijó, a pesar de la distancia temporal* [12]. Pero para que dicho documento sea jurídico debería estar destinado a crear, modificar o extinguir relaciones jurídicas, es decir, cuando el hecho que representa sea apto para generar consecuencias jurídicas.

En este sentido amplio de documento quedan encerrados los documentos electrónicos en la actualidad. Entiéndase que el concepto de documento

---

(9) Posición mantenida también por quien suscribe en el trabajo citado en la nota 2ª. Juan M. Alterini, "Prueba. Responsabilidad y Derecho Informático", *La Ley* 2003E. 1155.

(10) Prescribe al art. 1191 Cód. Civil: "Los contratos que tengan por objeto una cantidad de más de diez mil pesos, deben hacerse por escrito y no pueden ser probados por testigos".

(11) Betti, Emilio, "Teoría general del Negocio Jurídico", 2ª ed., *Revista del Derecho Privado.* Madrid, 1959 p. 106.

(12) Conf. Ghioldi, José Luis - Méndez, Guillermo Horacio, *Títulos de crédito*, Ed. De Belgrano, Buenos Aires, 1999, p. 22.

electrónico, hoy, incluye al correo electrónico y en general a la mayoría de las cuestiones radicadas en la Internet.

b) También debemos considerar la posibilidad de que –por distintos acontecimientos verificables– quien en principio tenía el *onus probandi* a su cargo se vea impedido de hacerlo. Nótese, por ejemplo, qué sucedería si un incendio destruyese la terminal de la cual fue enviado el mensaje. En dicho supuesto, sería eventualmente aplicable la teoría de las *cargas probatorias dinámicas* o la distribución de la carga de la prueba entre las partes, que fluye de los deberes de colaboración, buena fe y solidaridad que deben primar en el proceso.

Estos dos principios generales, el de la aplicación de la teoría de la prueba documental y la de las cargas probatorias dinámicas –en supuestos de excepción– no termina de conformar el régimen probatorio en el Derecho Informático. En efecto, a ellos debemos sumarles todo el régimen de la prueba indiciaria que establece tanto la ley de forma como la ley de fondo. Así, en lo que respecta al Proyecto de Código Civil de 1998, este régimen surge claramente del art. 296 [13].

Este criterio es conteste con el expresado en el artículo 9 de la Ley Modelo de UNCITRAL que brinda cuatro parámetros a los efectos probatorios: la autenticidad, la fiabilidad, la inalterabilidad y la accesibilidad de los documentos informáticos. Todos ellos receptados en la labor del legislador argentino [14].

c) Debería tenerse en cuenta el principio de la buena fe, que impregna a todo el Derecho positivo, y deja, en esta área, su lugar accesorio para tomar, al igual que en el Derecho del Consumo, una posición determinante. La buena fe, en lo que respecta al Derecho Informático, es determinante como primera concepción y, finalmente, como regla interpretativa que obliga a presumirla si se dan, como en el caso en comentario, los presupuestos que no la destruyan.

Ciertamente *"no resulta una tarea sencilla adecuar las normas civiles ni los principios generales del deber de responder a la tecnología puesto que, como se dijo, esta avanza mucho más rápido que el legislador. Por ello es el Poder Judicial quien tiene el desafío más importante. O bien se arraiga al sentido literal de las normas, o bien se desprende de ese arraigo y las interpreta"* [15].

Pero ello, que evidentemente constituye una tarea difícil, no lo es tanto si se considera que cuando se envía información mediante correo electrónico, el *recorrido* de éste por la Red queda registrado, no sólo en la computadora de la que salió sino también en los distintos servidores que le hayan permitido llegar al destinatario. Este *iter informático* queda en evidencia con el simple *clickeo* en la solapa "propiedades" del mensaje. De todos modos, no puede soslayarse que,

(13) Que textualmente dispone: "El valor probatorio de los instrumentos particulares debe ser apreciado por el tribunal ponderando, entre otras pautas, los usos del tráfico, las relaciones precedentes de las partes si las hubiere habido, y la razonable convicción que pueda alcanzarse sobre su autoría, legibilidad e inalterabilidad de acuerdo a los métodos utilizados para su creación y transmisión a terceros".

(14) Ley 25.506.

(15) "Prueba, Responsabilidad y Derecho Informático", *La Ley,* 2003 E, 1155.

en definitiva, la capacidad de traducción de los distintos códigos que surjan del mensaje dependerá de los distintos servidores y de su capacidad técnica.

Así las cosas y conforme a lo que sentenció la Excma. Cámara Nacional de Apelaciones en lo Civil, su Sala I, no parecería prudente apegarse al principio de *onus probandi incumbit actori* si, como lo dice el propio Tribunal, la respuesta técnica del servidor no pudo ser completada por la ausencia de información específica que se le requiriera precisamente al demandado.

Allí es donde la difícil tarea del juzgador se potencia y arroja un resultado reñido con el deber ser kelseniano: si la prueba fehaciente del instrumento particular no firmado –que hubiera servido como base al progreso de la acción– ha sido imposibilitada por la omisión de brindar información por parte del accionado, no parecería axiológicamente válido exonerar a éste de su responsabilidad.

Menos aún si cuando, como en el caso, la propiedad o, más precisamente, la titularidad de la cuenta de correo electrónico era de la cónyuge del accionado, lo que, a la luz de los principios reseñados, no permite concluir en la inexistencia del contrato. La prueba indiciaria, que, en conjunto, forma una presunción, no amerita, en el reseñado contexto [16] la eximición de responsabilidad, paradójicamente, por ausencia de prueba.

d) Por otra parte, y en lo que respecta a la ausencia de adecuada información por parte del servidor –debido a que el demandado no aportó la información requerida– pasa por alto que también aquél, el servidor, se encuentra comprometido a brindarla. Por ello *"quien ofrece dar 'hosting' en Internet anónimamente –en un 'sitio' por él creado y administrado– a toda persona que bajo cualquier denominación lo solicita para poner a disposición del público o de categorías de público, signos, señales, escritos, imágenes, sonidos o mensajes de cualquier naturaleza que no tiene el carácter de correspondencia privada, excede manifiestamente la calidad técnica de un simple transmisor de informaciones y debe asumir, respecto de los terceros cuyos derechos pudieran verse afectados en tales circunstancias, la consecuencia de una actividad que ejerce en forma remunerativa y con propósitos deliberados"* [17].

Conclusiones

De lo hasta aquí expuesto, entiendo que el fallo merece plausibles comentarios en lo que se vincula con el derecho de fondo. Se ha contextualizado en su justa dimensión al correo electrónico como un *instrumento particular no firmado.*

No concluyo de igual modo –y muy modestamente– en cuanto al aspecto procesal del tema, toda vez que se omitió considerar cuál es el régimen probatorio de tales instrumentos. Y, sin hesitación, se desestimó un planteo por

(16) Art. 163, inc. 5º, Código Procesal Civil y Comercial de la Nación.

(17) C.Apel. París, Sala 14, febrero 10 de 1999. "Haliday, Estelle c. Lacambre, Valentín", RCyS, 1999-1392.

ausencia de prueba que, en lo esencial, ha frustrado su producción el sujeto pasivo de la relación procesal [18].

Tampoco se concibió cuál era la obligación –incluso– que tenía el propio servidor como para no evitar brindar la información que hubiera elucidado la cuestión.

Es que tampoco puede omitirse –en términos de Cavanillas Mugica– que *"por la misma novedad de Internet y sus distintas formas de explotación, todavía no se han acuñado 'modelos de diligencia', aún no existe el canon de 'buen servidor' que equivalga al 'buen padre de familia'"* [19].

Pero, no debería haber dudas al respecto, el servidor de Internet, al asumir la prestación del servicio, se encuentra también precisado –por los principios generales del deber de responder– a obrar de manera diligente. Diligencia esta que, por definición, será imputable a modo subjetivo, y en grado de excepción, lo será de modo objetivo.

Al ser ello así, *"no se puede generalizar el principio de responsabilidad objetiva sino que debe estar limitado a ciertas áreas. Tampoco me parece correcto generalizar el principio de responsabilidad subjetiva, al estilo de los códigos socialistas, como el de Cuba de 1988. Si el Estado es el único que maneja los medios de producción, es evidente que no le va a convenir un régimen de responsabilidad objetiva. La excepción proviene de que se trata de una imputación con prescindencia de todo criterio de reprochabilidad, y eso tiene que suceder en determinadas áreas sin necesidad de que haya un solo factor de atribución, que pueden ser la culpa, el riesgo, la garantía, la solidaridad, la equidad. Diría que hasta el amor puede servir como factor de atribución de responsabilidad"* [20]. En suma, la contradicción entre los sólidos argumentos por un lado, y por otro, el apego a la literalidad de determinadas normas han coincidido en una erudita sentencia que, a la par, no ha interpretado, a mi modo de ver y con la cuota de artesanía que obliga la materia involucrada, la cuestión sometida a consideración.

---

(18) No se escapa que, como bien señala el Tribunal, había otros medios de prueba como para lograr certidumbre pero, lo cierto es que ello, en el contexto que refiere la sentencia, no era imputable o mejor dicho, esperable del actor.

(19) Cavanillas Mugica, Santiago, "La responsabilidad civil de los servicios de la sociedad de la información en la utilización de las nuevas tecnologías de la comunicación" en *Perfiles de la Responsabilidad Civil en el Nuevo Milenio*. Moreno Martínez, Juan Ambrosio: Coordinador, Dykinson, Madrid, 2000, p. 127.

(20) López Cabana, Roberto Manuel, "Análisis del Proyecto de Código Civil de 1998", en *Temas de Derecho Privado XII*, edición del Colegio de Escribanos de la Capital Federal, Buenos Aires, 2000, p. 53.