FIRMA DIGITAL - ANÁLISIS EXEGÉTICO DE LA LEY 25506/2001

(Ley 25.505 – Firma Digital. B.O. 14/12/2001)

Por Gabriel B. Ventura

INTRODUCCIÓN

La ley 25506, sancionada el 14 de noviembre de 2001 y promulgada el 11 de diciembre del mismo año, tiene por objetivo fundamental incorporar al derecho argentino la tecnología más avanzada hasta el momento, en materia de contratación a distancia; es decir la "tele contratación". Se basa en una moderna ténica de encriptación informática[1], que permite la remisión, vía internet, de documentos codificados, procurando con ello un cierto grado de certeza en cuanto a voluntad contractual y contenido del convenio. Merced a ello pueden atribuírsele efectos jurídicos plenos como manifestación de voluntad negocial y su consiguiente fuerza compulsiva.

Desde la antigüedad, en tiempos de guerra o paz, ha resultado todo un desafío la remisión de mensajes o correspondencia de manera segura, para impedir que la información caiga en manos ajenas al verdadero destinatario. Por ello podemos encontrar ejemplos, en tiempos remotos, de encriptación entre los espartanos, mediante la utilización de dos bastones simétricos llamados "scitalas", uno en poder del remitente y otro en poder del receptor. El remitente escribía su mensaje sobre un rollo de papiro que envolvía previamente en forma de espiras sobre la "scitala"; luego enviaba el rollo al receptor, a quien le bastaba con recrear el envoltorio sobre la otra

[1] "Encriptar" proviene de la voz griega "Kryptos" (ocultar) y "criptografía" de (oculto) y "gráphein" (escritura): Escritura oculta.

“scitala” simétrica a la anterior; es decir que respetaba el grosor y demás medidas de la “scitala” de origen. Se podía obtener así una lectura clara y segura del mensaje remitido[2] .

Con el tiempo, la “scitala” se sustituye por mecanismos lógicos matemáticos que permiten el descifrado de manera racional, atribuyendo el valor de letras a números o distintos valores a letras según el orden de colocación en las palabras o renglones. Nacen así los “algoritmos de encriptación”, cuyo conocimiento por parte del destinatario, permite una lectura sencilla y cierta a la par que impide el acceso a quien no tenga la clave o algoritmo para descifrar el mensaje. Pero siempre, como puede advertirse, en estos sistemas primitivos o primarios, se cuenta con un previo acuerdo entre remitente y receptor que es el “código de desencriptación”. Éste constituye o sustituye la vieja “scitala”. Este tipo de encriptación, en el que se cuenta con información previa en ambos polos de la comunicación (emisor y receptor) se denomina, justamente por ello “criptografía simétrica” y tiene la desventaja de admitir sólo comunicación entre dos o más partes, quienes han convenido previamente el pertinente código de desencriptación.

El avance de la informática en el mundo moderno permite sistemas más sofisticados aún, de encriptación mediante la creación de algoritmos cada vez más complejos, hasta llegar a los que, sin el apoyo de un ordenador, resultarían de imposible descifrado. Al mismo tiempo es también dicho avance el que ha posibilitado el hallazgo de un sistema llamado de “criptografía asimétrica” en la que ya no sería menester un previo conocimiento de la clave secreta del remitente.

En efecto, el gran hallazgo de la criptografía asimétrica lo constituye un procedimiento para lograr una comunicación segura y exclusiva con otras personas que justamente no tienen un conocimiento previo de la clave

[2] FARRÉS, Pablo; “Firma Digital”, Ed. Lexis Nexis, Bs.As. 2005, pág. 49.

secreta. Podríamos decir, si se nos permite la metáfora, que posibilita comunicación segura entre personas que no tienen la “scitala” gemela, de los espartanos, complementaria de un sistema simétrico. De ahí justamente su denominación “criptografía asimétrica”.

El sistema de criptografía asimétrica se logra asignando a cada usuario dos claves: una pública y otra privada. La pública se da a conocer por el usuario interesado en recibir información segura, en tanto que la privada queda sólo en su poder y debe ser cuidadosamente tutelada si se quiere mantener la privacidad y seguridad de sus recepciones y envíos[3].

Utilizando la clave pública del remitente cualquiera puede desencriptar su envío, que fue previamente encriptado mediante la clave privada del autor y “firmante”. La tecnología informática del sistema permite que lo encriptado con clave privada pueda desencriptarse mediante la clave pública e, inversamente, lo encriptado en la clave pública del receptor, pueda desencriptarse mediante su clave privada.

Sin embargo, nada podría lograrse sin la existencia de un intermediario en las comunicaciones, el llamado técnicamente “tercero de confianza”, cuya misión es verificar la autenticidad de cada envío. Toda remisión pasa previamente por una autoridad imparcial certificante que, justamente por ser su misión dar fe de la utilización de la clave privada del remitente y del destinatario, recibe el nombre de “certificador”, la gran vedette del sistema, y cuyas características surgen de lo normado en los arts. 17 al 23 de la ley bajo análisis.

---

[3] VENTURA, Gabriel B.; “Firma digital y documento notarial”, LL, 2004 -B, 1274. Decíamos ahí, criticando el sistema que “La firma sólo puede ser estampada por el titular, quien sólo mediante una situación de violencia compulsiva (vis relativa) podrá verse en la necesidad de estamparla involuntariamente. En cambio la digital puede llegar a conocimiento de terceros, sea por descuido, sea por manejo de la misma PC. en la que se encuentra grabada la firma digital. Todo operador de esa computadora podrá acceder a la firma. Será posible también la obtención de la firma digital mediante la violencia física o moral lográndose así una firma con todos los requisitos de autenticidad para el sistema digital”.

En Argentina, la firma digital se encuentra reglamentada en la ley 25506, sancionada el 14 de noviembre de 2001, promulgada de hecho el 11 de diciembre de 2001 y publicada el 14 de diciembre del mismo año. Su decreto reglamentario es el 2628 del año 2002. Tanto la ley, en un anexo final, como la reglamentación, por regular situaciones tan vinculadas a cuestiones técnicas, contienen un glosario de conceptos y definiciones que resulta de imprescindible lectura para comprender ciertos artículos de la ley. Hasta se prevé la posibilidad de fácil actualización de dicho glosario, sólo mediante decreto del ejecutivo, en los términos del artículo 99 inc. 2 de la Constitución Nacional, justamente para lograr la adecuación de la terminología legal a los acelerados avances tecnológicos e informáticos.

ART. 1 - OBJETO. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

En este artículo se determina cuál será el objeto de la ley, anunciando de manera categórica que la firma electrónica y la firma digital tendrán eficacia jurídica.

Recordemos que el código civil sienta como un principio paradigmático la necesidad de la firma ológrafa para que todo documento, tanto público como privado, tenga validez como tal. En efecto, en el art. 1012 del citado cuerpo legal se establece, como un principio rector, que la firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada, la que no puede ser reemplazada por signos ni por las iniciales de los nombres y apellidos[4].

[4] En la ilustrativa nota al art. 916 del Código Civil, Vélez Sársfield hace una pequeña pero clarísima doctrina acerca de la firma, cuando expresa que “Desde la Edad Media, dice Savigny, la declaración escrita se hace poniendo el nombre propio debajo de un acto

También respecto de los instrumentos públicos se sienta ese mismo principio en el artículo 988 del Código Civil, cuando se determina que el instrumento público requiere esencialmente para su validez, que esté firmado por todos los interesados que aparezcan como parte en él. Otro tanto surge del art. 1004 para las escrituras públicas en particular. En consecuencia, la falta de firma en los instrumentos públicos determina, según las normas citadas, su nulidad instrumental[5].

Pues bien, en su primer artículo la ley bajo análisis, mediante este pronunciamiento previo, modifica o al menos retoca, a estos efectos, el citado art. 1012 del Código Civil, adjudicando plena eficacia también a la firma electrónica y firma digital, tal como se determinará de manera contundente en el artículo 3, según veremos.

La doctrina ha criticado la expresión "firma digital" utilizada por el legislador, dado que esas palabras limitan su aplicación sólo a un sistema de encriptación fundado en la digitalización binaria, siendo que es muy probable que, en un futuro no muy lejano, puedan llegar a utilizarse otros procedimientos de identificación de autenticidad, como por ejemplo a través de la lectura del iris de las partes contratantes. Era preferible utilizar, según Farrés, sólo la expresión "firma electrónica", dado que la energía y los

---

escrito, y la firma establece que el acto expresa el pensamiento y la voluntad del que lo firma. El acto no valdría por el derecho moderno aunque estuviese escrito por la parte, si no estuviese también firmado". Más adelante, al regular el testamento ológrafo, en nota al art. 3639, expresa que "La firma no es la simple escritura que una persona hace de su nombre y apellido; es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esa formalidad. Regularmente la firma lleva el apellido de la familia; pero esto no es de rigor si el hábito constante de la persona no era firmar de esta manera. Los escritores franceses citan el testamento de un obispo, que se declaró válido, aunque la firma consistía únicamente en una cruz seguida de sus iniciales, y de la enunciación de su dignidad".

[5]Cuando las normas citadas aluden a la "falta de firma de las parte", se refiere a "partes" en el sentido instrumental no sustancial. Por ello la falta de firma de cualquiera de los comparecientes, aunque no sea de una de las partes del contrato, anula el acto, aun respecto de las partes que lo hubieren firmado (artículo 988 del Código Civil). Las normas pues aluden a la forma y no al contenido negocial.

impulsos eléctricos tienen un mayor futuro en cuanto a que seguirán siendo, por mucho tiempo, la base de todo sistema[6].

ART. 2 – FIRMA DIGITAL. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

En este dispositivo el legislador procura brindar una definición de firma digital, al que refiere como un "procedimiento matemático", que desde el punto de vista informático realiza automáticamente el ordenador. Se da por supuesta la existencia de un documento electrónico; es decir digitalizado o informatizado por el procedimiento que fuere, que será el documento al que se aplicará la "firma digital". La misma ley define luego, en el artículo 6 el documento digital.

La firma digital consiste básicamente en un algoritmo matemático que utiliza dos claves, tal como ya habíamos expresado, una pública y otra privada. Estas claves serán creadas por el mismo usuario "firmante", en su propio ordenador mediante herramientas del sistema. La clave privada que

[6] FARRÉS, Pablo; "Firma Digital", Ob.Cit., pág. 52.

es de uso exclusivo del firmante y la clave pública que es la que se da a conocer a los terceros y acompaña al documento firmado[7].

Para que un sistema de contratación a distancia pueda resultar efectivo jurídicamente hablando, es necesario que pueda acreditarse de manera indubitada la identidad del firmante y la correspondencia entre el texto suscripto y la voluntad del mismo. Para que esa vinculación resulte indiscutible se hacen menester estos procedimientos matemáticos complejos que, mediante la encriptación por el iniciador y desencriptación en destino, permiten concretar esta función tuitiva.

Pero para lograr la generalización del uso de un sistema de contratación a través de redes informáticas, es necesario brindar la seguridad de ciertos elementos. Es lo que en tecnología informática se designa con la expresión técnica “confianza digital”.

Generar la confianza digital, será la única manera de lograr que el sistema se generalice en su utilización. En tal sentido puede reprocharse al dispositivo no haber hecho hincapié en otras características fundamentales que debe brindar la firma digital para brindar esta forma de negociación de la que venimos hablando.

La doctrina tiene analizadas cuáles serían esas condiciones básicas para lograr una contratación electrónica segura. Así, se ha puesto énfasis en seis características fundamentales que brindan seriedad jurídica a un sistema de firma que permita una contratación electrónica seria. Debe tener confidencialidad, integridad e inalterabilidad, autenticidad; que no admita

[7] GIRAL FONT, Martín J.; “Certificación Notarial de Firma Digital”, en Revista Notarial, Nº 879, pág. 278.

repudio arbitrario que brinde fecha cierta; y que, por todo ello, genere un vínculo jurídico conminable[8].

Cuando se establece que el sistema debe ser **confidencial**, se exige que no pueda tener acceso a la información quien no será parte de la negociación o acuerdo. La penetración de terceros en el intercambio de mensajes e información ha sido un tema preocupante desde que las redes informáticas comenzaron a utilizarse en forma masiva. Este efecto de privacidad se logra mediante la encriptación del mensaje a través de algoritmos matemáticos cifrados mediante el procedimiento binario. De esta manera si alguien tuviere acceso al mismo, al no tener la clave de desencriptación, no podrá acceder a la información del documento ni alterar su contenido. Por otra parte si lograse modificarlo antes de que éstos lleguen a destino, dicha modificación quedará denunciada al desencriptarse el documento electrónico, lo que confiere al sistema otro de los recaudos necesarios para generar confianza, la **integridad e inalterabilidad**; es decir la certeza en cuanto a que la expresión de voluntad del cocontratante, plasmada en el documento original, no ha sido modificada y que realmente se ha querido contratar en las condiciones en que el documento lo indica con verdadero "animus signandi". Esta posibilidad técnica repercute en la presunción "iuris tantum" sentada en el artículo 8 de la ley 25506.

También será necesario que mediante la utilización del sistema pueda identificarse al firmante y garantizarse así que el cocontratante sea quien debe ser, lo que constituye la **autenticidad** de la firma; es decir la correspondencia entre el sujeto firmante y su verdadera voluntad. Esto es fundamental para que no pueda repudiarse, de lo contrario no podría generar efectos jurídicos permitiendo conminar su cumplimiento. Ni el

[8] LUZ CLARA, Bibiana; "Ley de firma digital comentada", Ed. Nova Tesis, 2000, Rosario, pág. 41. KATZ, Flora M. "El notariado. El comercio electrónico. Firma digital", Revista del Notariado, Bs.As. 2004, Nro. 878, pág. 303.

remitente podrá válidamente esgrimir que no ha enviado ese mensaje, ni el destinatario podrá negar haberlo recibido, generándose así el vínculo obligacional característico de todo contrato. De tal posibilidad técnica surge la presunción de autoría y recepción determinada en los artículos 7 y 10 de la ley que comentamos. Obviamente estas presunciones son "iuris tantum".

Trabajan en este concepto las básicas normas de los artículos 1144 y 1147 del Código Civil[9]. En efecto el artículo 1144 establece que "El consentimiento debe manifestarse por ofertas o propuestas de una de las partes, y aceptarse por la otra" y el 1147 determina que "Entre personas ausentes el consentimiento puede manifestarse por medio de agentes o correspondencia epistolar". Sin dudas el sistema de contratación electrónica no escapa a estos básicos pronunciamientos de las normas transcriptas.

En cuanto al momento preciso de formación del consentimiento mediante la firma digital, así como la fecha cierta, tanto entre partes como "erga omnes", regulada genéricamente en los artículos 1034 y 1035 del Código Civil, lamentablemente la ley 25506 no contiene dispositivo alguno que la determine, en razón de lo cual, y en aplicación de la doctrina que rige en el derecho común, podrían aplicarse alguno de los cuatro clásicos sistemas propuestos para la regulación de la oferta y la aceptación: el momento de la declaración, el de la expedición, el de la recepción y el del conocimiento[10]. Pero debe remarcarse que, la existencia de la fecha cierta de cada uno de esos casos sería imprescindible, y el no haberle dado dicho carácter a algún momento determinado, pone dudas sobre su determinación[11]

---

[9] MOLINA QUIROGA, Eduardo; "Documento y firma electrónicos o digitales", La Ley, 2008 - F, pág. 1084.

[10] MOISSET DE ESPANÉS, Luis y MARQUEZ, José F. "La formación del consentimiento en la contratación electrónica", LL, 2004 - F, pág. 1183.

[11] FARRÉS, Pablo; Ob.Cit. pág. 112, dice: "El servicio de timbre fechador no ha sido equiparado por la ley 25506, en sus efectos, al de fecha cierta, carece de toda presunción legal asignada (...)".

Con el avance de las ciencias y la técnica podrán surgir nuevos procedimientos que habiliten un sistema tanto o más seguro que los actualmente conocidos; por ello, con buen criterio, la norma alude en su último párrafo, a la necesidad de que la Autoridad de Aplicación los determine “(...) en consonancia con estándares tecnológicos internacionales vigentes”. Sin duda esta posibilidad prolonga la vida útil de la ley al permitir la rápida adecuación de sus normas a los avances de la ciencia.

ART. 3 - Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

Esta norma procura, de una manera demasiado facilista en nuestra opinión, ensamblar la firma digital a todo el derecho positivo vigente. Cuando alude a ley, en abstracto, se refiere fundamentalmente al derecho común, es decir al Código Civil; pero también se involucra en el dispositivo cualquier ley especial que regule instrumentos públicos o privados. Así las leyes que regulan los títulos valores, los contratos especiales, las declaraciones juradas, y demás formularios comerciales o administrativos entrarían “prima faccie” dentro de esta lacónica remisión que, de nuestra parte nos parece exagerada. Por ello en la norma siguiente, con prudencia y buen criterio, se sienta lo que será, a no dudar, el principio rector para juzgar la aplicabilidad de la firma digital. Adviértase que las excepciones a la norma del artículo 3, sentadas en el artículo 4, son tantas y tan genéricamente redactadas que dejan fuera del sistema, a pesar del entusiasmo de sus operadores, casi todos los actos más importantes de la vida civil.

Recordemos que para el Código Civil la firma resulta ser un elemento esencial para la validez de todo acto bajo forma privada, ya que no puede reemplazarse por signos o iniciales, tal como lo establece de manera contundente en su artículo 1012. En tanto para los instrumentos públicos se condena también con nulidad instrumental absoluta, los que adolecieren de las firmas de las partes: artículos 988, para los instrumentos públicos en general y 1004 para las escrituras públicas en particular.

Sin dudas el artículo 3 de la ley 25506 que estamos comentando, modificaría en primer lugar estos dispositivos, salvo por la aplicación de las mismas excepciones sentadas en el artículo 4 de la ley 25506 a las que ya hemos hecho referencia. En el caso de las escrituras públicas, dado la contundente exigencia de estar en el protocolo establecida en el artículo 998 del Código Civil, quedarían fuera del ámbito del artículo 3 que estamos analizando.

Otro tanto ocurre con el artículo 916 del Código Civil y su nota, y los artículos 988 y 1004 que exigen la firma para que el documento no presente nulidad instrumental.

Pues bien, este art. 3 aplica la fuerza vinculante de la firma ológrafa a la llamada “firma digital”; pero debe remarcarse que el concepto de ésta, aun desde el punto de vista jurídico, de firma tiene poco. Debería asignársele la expresión “signo”, “código”, o “pasword”, pero no firma.

Las leyes van destinadas al vulgo, al hombre común, a los legos, y la idea de la firma puesta al pié, siguiendo las acotaciones de Vélez en la nota al art. 916 del Código Civil citado, así como toda la regulación referida a ella en los arts. 1012 y siguientes del Código Civil, de llamarle firma al signo codificado previsto en la ley 25.506, hará que se apliquen erróneamente respecto de ese código toda la normativa reguladora de la firma y ello, en nuestra opinión, no es correcto. Por ello decíamos que la expresión del

artículo 3 era exagerada. Estimamos que la claridad que debe existir en las leyes hubiere exigido que la 25506 hubiere comenzado expresando que por este sistema legal, en algunos casos, no será menester la firma y que para vincular jurídicamente a dos partes, sólo en esos casos, bastará con los signos o códigos que garanticen la autoría y procedencia[12].

ART. 4 - Exclusiones. Las disposiciones de esta ley no son aplicables:

a) A las disposiciones por causa de muerte;

b) A los actos jurídicos del derecho de familia;

c) A los actos personalísimos en general;

d) A 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.

En el art. 4 de la ley 25.506 se excluyen de aplicación de la firma digital ciertos actos que, por su especial naturaleza, ha obligado a cierta prudencia al legislador. Más allá de las críticas que pueden efectuarse al dispositivo, algo de lo cual poníamos de resalto al analizar el artículo 3, en cuanto a que serían más las excepciones que las reglas, sin dudas los motivos del legislador para excluir estos actos aquí enunciados obedece a los siguientes motivos: En primer lugar, aunque no confesada, la falta de convencimiento respecto de la seguridad del sistema. En segundo lugar el hecho de que el verdadero aporte de la firma digital es la celeridad en la

[12] VENTURA, Gabriel B. “Firma digital y documento notarial”, Ob.Cit.

negociación y, en los actos enunciados, excepción hecha de los contenidos en el último inciso en algunos de los cuales podría sí existir dicho imperativo, esa necesidad aparece en un segundo plano.

Las expresiones poco técnicas del legislador, en esta norma, hacen que, en nuestra opinión, los tres primeros incisos pueden subsumirse en uno sólo. En efecto, tanto las disposiciones por causa de muerte, como los actos de derecho de familia en general, deberían considerarse como “actos personalísimos” a los que alude el inciso “c”. Debe tenerse presente que los actos personalísimos no tienen un enmarque legal preciso. Ni siquiera sería factible elaborar una enumeración de tales actos ya que ese supuesto carácter dependerá de muchos factores. Mientras algunos podrían considerar en su concepto los actos que involucran derechos extrapatrimoniales personalísimos, como lo serían la patria potestad, el nombre y hasta el aspecto moral del derecho intelectual; otros simplemente consideran personalísimos los derechos extrapatrimoniales. Pero tampoco faltarán, por otra parte quienes atribuyan dicho carácter a los contratos que obliguen a prestaciones que sólo puedan ser cumplidas por ciertas personas, como lo serían la realización de piezas artísticas o científicas en las que el autor resulta ser uno de los principales motivos determinantes de la contratación (Ej. un contrato con un artista plástico reconocido para retratar a una persona).

Pero amén de la prudencia puesta de manifiesto, al excluir algunos actos, que en este punto y con las salvedades del caso es elogiable; se pone de resalto en esta norma, que ni los propios autores del sistema, informáticos, legisladores y en general, se atreven a suponer la seguridad total del sistema.

Estimamos que, en seguimiento de esta norma, las disposiciones de la ley no se podrán aplicarse a los testamentos, para lo cual seguirán rigiendo con exclusividad las normas de los arts. 3639, 3658 y 3666 del

Código Civil; ni se aplicarán tampoco a los actos jurídicos relacionados con el derecho de familia: celebración de matrimonios, reconocimientos de hijos, impugnación de paternidad, etc. No serán aplicables igualmente, las firmas digitales, a los actos relacionados con los derechos personalísimos en general: donación de órganos; autorizaciones relacionadas con derechos intelectuales; con el nombre de las personas, etc.

No podemos dejar de considerar también excluidos de la aplicación de la ley 25506, por aplicación del inciso "d" de la norma analizada, los actos que deben celebrarse en escritura pública. En efecto, en el último inciso del art. 4 de la ley 25.506 se agrega un dispositivo bastante amplio que excluye todos los actos que "[...]deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposicioens legales o acuerdo de partes". Ya en otras oportunidades hemos expresado que en este inciso está presente la escritura pública[13]. Todos los actos que exigen dicha forma instrumental estarán excluidos de la aplicación de los dispositivos de la ley 25506.

Los motivos de dicha exclusión resultan obvios si recordamos las exigencias del art. 1001 y todos los recaudos formales previstos en especial en los arts. 988, 989, 1001, 1004 y 1005 del Código Civil que pasarían a tener el directo efecto excluyente de la ley bajo análisis. A manera de ejemplo (la norma principal) el art. 1184 con sus once incisos[14].

El requisito del protocolo[15], típico de un sistema notarial latino, coloca otro obstáculo más a esta aparente "evolución" de la forma contractual. La exigencia de que el acto notarial deba estar en el protocolo y en la página que corresponda según su fecha (art. 998 y 1005 del C.C.), bajo pena de

[13] VENTURA, Gabriel B.; "Firma Digital" Ob. Cit.

[14] En este aspecto esta ley resulta mucho más prudente que el art. 266 y 268 inc. e) del Proyecto de Modificación global del Código Civil.

[15] El protocolo, cuya expresión proviene del latín "protocollum" (primer ejemplar encolado), exige un título matriz y un original con valor ejecutivo, según expresa Vélez citando antigua legislación española (nota al art. 997 del C.C.). En ese sentido resulta también incompatible con lo surgido del art. 11 de la ley 25506.

nulidad instrumental, impide por completo la aplicación de la firma digital a dichos actos[16].

En cuanto a la certificación notarial de firmas ocurre otro tanto, ya que las leyes orgánicas notariales exigen, en general, los mismos recaudos formales para estos actos que para las escrituras públicas[17].

ART. 5 - Firma Electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

Tanto desde el punto de vista jurídico como técnico hay una diferencia de grado entre la firma digital y la firma electrónica. Esta última es el género, mientras que la firma digital, al resultar más rigurosa en sus recaudos, aparece como una versión perfeccionada o "modelo avanzado" de firma electrónica. La doctrina considera, que la inserción de esta norma en la ley 25506, obedece a la necesidad de dotar al sistema jurídico positivo de un mecanismo que permita incluir los nuevos avances tecnológicos que se puedan ir dando en la materia; pero que aún no pueden brindar la seguridad requerida para asignarle el efecto vinculante inmediato.

La diferencia de grado que expresábamos más arriba, hace alusión al valor probatorio que la ley le asigna. Así, mientras la firma digital prueba con

[16] Tener presente que todas las nulidades instrumentales son nulidades absolutas y, como tales, inconfirmables. Ver al respecto VENTURA, Gabriel B. "La ley 17.801. Registro de la Propiedad Inmueble Comentada. Anotada", Ed. Hammurabi, Bs.As. 2009, pág. 150 a 152.
[17] Así, a modo de ejemplo, el art. 13 de la ley 4183 Orgánica del Notariado de Córdoba.

carácter “juris tantum”, luego de recabados los certificados respectivos, de la existencia de la firma, el acuerdo con el contenido, su procedencia y el “animus signandi”; la firma electrónica sólo aporta un elemento probatorio al que deberán agregarse otros géneros acreditativos para llegar recién a generar el vínculo jurídico. Si se trata de una firma digital, quien la niegue deberá probarlo; si se trata de firma electrónica el que la aporta debe probar su autenticidad, procedencia e inalterabilidad para que recién se genere el vínculo jurídico.

Es decir, parafraseando el lenguaje técnico usado para los documentos en soporte papel, la firma electrónica generará un “principio de prueba por escrito”, a la manera de los documentos particulares a los que hace referencia el artículo 1190 del Código Civil y 1192, segundo párrafo. Mientras la firma digital garantiza confidencialidad, integridad, e imposibilidad de repudio injustificado[18], según habíamos analizado en nuestro comentario al artículo 2 de esta ley, la firma electrónica en cambio no asegura estas prestaciones. Remarquemos que no es que no las tenga, sino que no puede garantizarse prima faccie que las presente.[19]

Gracias a este dispositivo deben considerarse incluidos como sistemas de identificación de firmantes, o sea como firma electrónica, por ejemplo, la firma ológráfica digitalizada sobre un documento electrónico; o una clave secreta de seguridad que accede a un sistema informático; o la lectura digital del iris o las huellas dactilares de los firmantes[20].

No podemos dejar de reprochar al legislador el hecho de haberle dado nacimiento o reconocimiento a la firma electrónica y retacear luego su reglamentación. El artículo que comentamos es el único dispositivo que

---

[18] KATZ, Flora M. “El notariado. El comercio electrónico. Firma digital”, Revista del Notariado, Bs.As. 2004, Nro. 878, pág. 303.
[19] MARQUEZ, José F. y MOISSET DE ESPANÉS, Luis; “La formación del consentimiento…” Ob.Cit.
[20] LUZ CLARA, Bibiana; Ob.Cit. pág. 47.

alude a ella. Se advierte la necesidad de haber regulado sobre todo lo que respecta a las responsabilidades que pudieran generarse frente a daños concretos, tal como lo pone de resalto Farrés[21]

ART. 6 - Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

Tanto la palabra “documento” como “instrumento” tienen el mismo significado, pues ambas derivan de expresiones equivalentes. Documento deriva del verbo latino “docere” enseñar; e Instrumento deriva de “instruo” que significa instruir. Ambas expresiones pues, aluden al efecto de dar a conocer algo o enseñar algo. Por ello nos resultan vanas las lucubraciones que suelen efectuarse procurando diferenciar “documento” de “instrumento”. Sin dudas desde el punto de vista jurídico resultan sinónimos. La ley que comentamos ha utilizado la expresión documento digital y entendemos que debe ser interpretada como sinónimo de “instrumento digital”.

En cuanto a la expresión legal, corresponde sin embargo aclarar que el documento digital es una especie de documento electrónico que resulta la expresión más adecuada para generalizar el fenómeno. Así diríamos que todo documento digital es documento electrónico; pero no todo documento electrónico es documento digital, ya que para que exista aquél es menester tan sólo que sea generado por medios electrónicos, en tanto que éste exige la digitalización que consiste en una secuencia informática de “bits” Es

[21] FARRÉS, Pablo, Ob.cit. pág. 347.

creado mediante la utilización de un ordenador mediante técnicas informáticas[22].

Recordemos que el Código Civil expresamente regula en materia de forma, la necesidad de que queden por escrito ciertos contratos en relación a los valores en juego. Así, en el artículo 1193 determina que "Los contratos que tenga por objeto una cantidad de más de diez mil pesos, deben hacerse por escrito y no pueden ser probados por testigos". Obviamente la ley se está refiriendo al soporte papel que es el tradicionalmente evocado por cuantas leyes aluden a "contrato escrito" por oposición al contrato verbal. Pero el avance de la ciencia y la técnica permiten hoy otro tipo de soportes, y probablemente aparecerán más variantes en lo futuro.

Así tanto el soporte magnético a través de cintas o discos, o el soporte "láser" (óptico) y las distintas combinaciones de estos sistemas, nos dan la posibilidad de contar con el soporte informático que trabaja con el sistema de numeración binario. Justamente la expresión digital proviene de la utilización de dígitos (números) para la primaria expresión en el ordenador; es decir asignando ceros y unos de manera combinada. La información así contenida, sería un documento digital que a su vez puede estar archivado directamente en el ordenador, en su memoria; enviado por correo electrónico a otros ordenadores, o ser extraído mediante la utilización de distintas técnicas, sean los discos compactos, los micro discos magnéticos, etc. Por ello la ley expresa que es indiferente el soporte usado para su fijación, archivo o almacenamiento.

Mientras estos nuevos soportes documentales cuenten con recaudos mínimos de seguridad, en cuanto a su resguardo e inalterabilidad, y resulten indelebles, pueden hacer su aporte al llamado "derecho documental"

[22] LUZ CLARA, Bibiana; Ob.Cit. pág. 51. MOLINA QUIROGA, Eduardo; "Documento y firma electrónicos o digitales", La Ley 2008 - F, 1084.

incorporándose en su materialidad a la categoría de medios de fijación. La duda que nos queda, porque no se hace fácilmente perceptible, es si realmente estos documentos no pueden ser alterados sin dejar una clara huella de su modificación; es decir si resultan realmente indelebles. En ese sentido creemos que el soporte papel constituye, aun hoy, el elemento más seguro.

Tal como habíamos expresado al comentar la definición de firma digital, en relación al artículo 2 de la ley 25506, este sistema da por supuesto el documento digital, puesto que es a él al que se aplica la firma digital con efecto vinculante en lo negocial, por ello la ley, con acierto, define su alcance de manera precisa y a la vez con la amplitud necesaria en estos casos tan relacionados con el avance de la ciencia, de lo contrario el dispositivo quedaría obsoleto quizás tan sólo en algunos meses.

El pronunciamiento final del artículo 6 que comentamos, relaciona el documento digital con toda la normativa, tanto civil como comercial o administrativa, que exige la expresión por escrito como forma instrumental.

ART. 7 - Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

Esta norma nos resulta de particular trascendencia, dado que se fija aquí el principal efecto jurídico de la firma digital. Se presume “iuris tantum”[23] la “autoría” del mensaje; es decir que la firma es auténtica y por ende el contenido documental resulta ser la verdadera manifestación de la voluntad

[23] FARRÉS, Pablo; Ob.Cit. pág. 113.

del firmante[24]. Junto con el certificado digital reglamentado a partir del artículo 13, ese documento digital generará todos los derechos y acciones que normalmente concede un documento al titular de los derechos en él contenidos, para probarlos y ejecutarlos por vía conminatoria de ser menester a través de la Justicia, salvo que el ejecutado pruebe que ha habido algún procedimiento que alteró el normal desenvolvimiento del sistema y la firma no le pertenece o el documento ha sido alterado. Pero mientras esta pruebe no se plantee exitosamente la acción prosperará.

Como puede advertirse el efecto aquí consignado, coloca al documento digital firmado en una situación intermedia entre el instrumento público y el instrumento privado, según la regulación establecida en el Código Civil. Mientras el instrumento privado en el Código sólo genera vinculo jurídico una vez reconocida la firma, o dada por reconocida, según lo determina el artículo 1026 C.C., para lo cual el firmante está obligado a prestar esa declaración en sede judicial en caso de serle requerida, a tenor de lo previsto en el artículo 1031 del Código Civil; el documento digital debidamente firmado con las previsiones de la norma que analizamos, genera ya el efecto jurídico invirtiendo “onus probandi”, en razón de lo cual, sólo caería la presunción de autoría frente a la prueba en contrario. No es menester el reconocimiento previo.

En cuanto al instrumento público comienza por probarse a sí mismo (“scripta pública probant se ipsa”) y luego, conforme a la tabulación establecida en los artículos 994 y 995 prueba también, con distintos grados de fuerza, respecto de su contenido. Quien quiera desconocer la autenticidad de un instrumento público deberá impugnarlo por nulidad

[24] Resulta de especial importancia para analizar el efecto jurídico vinculante de la firma, la breve referencia que hace Vélez Sársfield en la nota al artículo 916 del Código Civil, cuando expresa que “Desde la edad media, dice Savigny, la declaración escrita se hace poniendo el nombre propio debajo de un acto escrito, y la firma establece que el acto expresa el pensamiento y la voluntad del que lo firma. El acto no valdría por el derecho moderno aunque estuviese escrito por la parte, si no estuviere también firmado. (…)”

instrumental (artículos 980, 985, 986, 988, 993, 998, 1004, 1005, entre otros del Código Civil), según los casos. Para desconocer, en cambio la autoría de un documento digital bastará la simple prueba en contrario.

ART. 8 - Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de la firma.

Como habíamos expresado respecto a los recaudos de seguridad que debía presentar el sistema, al analizar el concepto de firma digital en nuestro comentario al artículo 2 de esta ley, debe tener entre otras virtudes lo que habíamos calificado de inalterabilidad que, junto a la confidencialidad, autenticidad y no repudio, generará, un vínculo jurídico conminable y ejecutable a través de la justicia[25].

La **integridad e inalterabilidad** podría definirse como la certeza o el grado de certeza en cuanto a que la expresión de voluntad del cocontratante, o declaración plasmada en el documento electrónico, no ha sido modificada y que realmente se ha querido contratar en las condiciones expresadas en el texto del mensaje. La posibilidad técnica que brinda el sistema posibilita la presunción “iuris tantum” sentada en la norma que comentamos y que, en la práctica, implica la inversión del “onus probandi”.

[25] LUZ CLARA, Bibiana; “Ley de firma digital comentada”, Ed. Nova Tesis, 2000, Rosario, pág. 41. KATZ, Flora M. “El notariado. El comercio electrónico. Firma digital”, Revista del Notariado, Bs.As. 2004, Nro. 878, pág. 303.

Es necesario destacar que lo único que esta presunción de autenticidad, integridad e inalterabilidad, no implica necesariamente que el instrumento se transforme en instrumento público, como se han atrevido algunos a sostener[26]. Ni las normas de los arts. 993 a 995, ni la doctrina elaborada en torno al valor probatorio de los instrumentos públicos, resultará aplicable al contenido documental. Adviértase que hacer semejante sinonimia, si se nos permite la expresión, implica desprenderse del trámite de redargución de falsedad previsto en el artículo 993 del Código Civil, así como todo lo referido al valor probatorio de las menciones dispositivas (artículo 994 C.C.) y enunciativas directas o indirectas (artículo 995 C.C.). La expresión del legislador no ha sido tan dañina, como sí pretende serlo la doctrina. Lo único que el legislador ha querido en el artículo 8 es invertir el "onus probandi", para que el supuesto firmante, una vez verificada digitalmente su firma, sea él quien deba probar que no es su firma o que se ha cambiado su contenido. Pero a ello se llegará con simple prueba en contrario, lo que no bastaría si se tratara de un instrumento público, en el que se haría menester el trámite de la redargución de falsedad previsto sustanciadamente en el artículo 993 del Código Civil. y procedimentalmente en el artículo 335 del Código Procesal de la Nación. Este trámite sería menester, ineludiblemente, para impugnar un instrumento público.

El artículo 8, en cuanto a sus efectos, ni siquiera equivale a una firma holográfica certificada, situación en la que la firma y el acta notarial respectiva redactada en el libro de certificación de firmas, son instrumentos públicos y por ello, para ser agredidas en cuanto a su veracidad y autenticidad, deberán ser impugnadas por redargución de falsedad. El repudio de la firma digital no exige tanto, bastará la simple prueba en contrario ya que juega a su favor la presunción de la autoría.

[26] WEINGARTEN, Celia; "Informatización y Firma Digital", La Ley, 2005-A, 1072.

ART. 9 - Validez. Una firma digital es válida si cumple con los siguientes requisitos:

a) **Haber sido creada durante el período de vigencia del certificado digital válido del firmante;**

b) **Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;**

c) **Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.**

Como ocurre en el derecho común, cuando se regula la vinculación negocial de los sujetos mediante documento en soporte papel y firma ológráfica, en esta norma se exigen condiciones de validez. Pero debe tenerse presente que no se alude a la validez del acto en sí, sino sólo se refiere a la firma. Obvio es que si la firma no es válida también caerá el documento portante del acto y acto mismo. El artículo nos evoca comparativamente las normas de los artículos 988 y 1004 del Código Civil, en materia de instrumentos públicos en general y escrituras públicas en particular; así como el art. 1012 para los instrumentos privados. Sabemos que estos dispositivos del Código Civil regulan lo atinente a la validez formal del documento y, consecuentemente uno de los recaudos de validez del acto; pero esto último, como decíamos, sólo como consecuencia del primer pronunciamiento.

Por ello la norma del art. 9 debe ser interpretada y aplicada con todo rigor sólo al valor de la firma en sí; pero cuidando de no hacer extensivo dicho pronunciamiento al documento digital al que se aplica ni mucho menos al acto que guarda; dado que, como toda manifestación de voluntad, será pasible de agresión por otros mecanismos de impugnación, que no escapan al derecho común; como la nulidad o la falsedad, por cualquiera de los motivos que se hicieran procedentes.

Entendemos que la enumeración contenido en este artículo es taxativa, o al menos tiene vocación de tal, ya que si bien el legislador no se pronuncia sobre ello, aparece *prima faccie* conteniendo todos los supuestos que pueden presentarse en relación a la firma en sí. Consecuencia de esta apreciación, sólo será factible impugnarla por nulidad si no se cumplen algunos de los incisos de la norma que estamos analizando.

Sin embargo, encumbrada doctrina, adentrándose en lo sustancial del negocio, adjudica carácter ejemplificativo al dispositivo, dado que encuentra en la nulidad sustancial, los otros supuestos que negarían validez a la firma, así como la posible alteración del texto documental base del negocio o acto jurídico firmado digitalmente. Por ello leemos en Farrés que si bien la norma menciona algunos de los motivos que anulan la firma, "(...) no necesariamente son los únicos. Existen otros, como la capacidad de los sujetos recaída dentro del período de validez de un certificado, la evidente alteración o defecto de transmisión del mensaje o su almacenamiento (...)"[27].

Sin dudas, en esta apreciación se han cometido dos errores; en primer lugar confundir la firma con el documento electrónico al que se adosa; y en segundo lugar, la no diferenciación de la nulidad instrumental con la sustancial, que tan claramente marca Vélez en los arts. 1044 y 1045 del Código Civil. Se están aplicando erróneamente supuestos de nulidad del

[27] FARRÉS, Pablo; Ob.Cit. pág. 124.

acto suscripto mediante firma digital, a la validez de la firma misma. En efecto, aunque la firma sea válida si el acto resulta nulo no habrá negocio jurídico eficaz; pero ello no obedece a la nulidad de la firma. Igualmente otro tanto podemos decir en el caso en que el mensaje haya sido modificado; la firma será válida, pero el contrato resultará ineficaz para generar el vínculo jurídico; dado que la manifestación de voluntad ha sido alterada y detectada exitosamente dicha alteración por los mecanismos informáticos del sistema[28].

La norma se refiere fundamentalmente a los certificados digitales, mencionados en cada uno de los tres incisos de la norma que analizamos, y cuya regulación se aborda a partir del artículo 13 al 16 de la ley 25506. Entendemos por certificado digital un documento electrónico cuya finalidad es confirmar y garantizar la identidad del firmante de un documento digital y su vinculación con el mismo. En definitiva es el elemento determinante del efecto vinculante válido de la firma con un acto o hecho jurídico. Por ello el artículo 9 necesariamente se refiere a los certificados al pronunciarse sobre la validez de una firma digital. Analizamos cada inciso del art. 9 por separado:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante: El documento digital tiene un plazo de validez que debe estar expresamente indicado en el mismo, según lo exige el art. 15 de la ley 25506, de manera tal que ambos polos de la relación jurídica pueden recabar este importante elemento de validez documental, asegurándose así el cumplimiento de este recaudo formal[29].

---

[28] Es el carácter de intangibilidad que se aplica a la firma digital en cuanto a que impide la modificación indetectable del documento suscripto digitalmente. Si no existiera dicha posibilidad de corroboración, el sistema sería inseguro y caería prontamente en desuso. Ver nuestro comentario al artículo 2.

[29] LUZ CLARA, Bibiana; dice: “La información sobre los certificados digitales debidamente actualizada debe permanecer *on line* para su consulta por los interesados en el momento

b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente: Esto quiere decir que la firma no tendrá validez si antes no ha sido verificada por el certificador y, obviamente ha sorteado con éxito dicho proceso.

c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de esta ley, por un certificador licenciado: Se exige que el certificado haya sido emitido por un certificador licenciado, cuyas exigencias surgen del art. 14 de la ley 25506; pero la redacción de la norma, en nuestra opinión, presenta un error sintáctico que dificulta su interpretación. En efecto, por haber insertado la coma (“,”) después de la expresión “reconocido”, habría quedado como si la norma sólo se refiriese a los certificados extranjeros, pues determina que debe serlo según el artículo 16 que se refiere a los mismos. Por ello estimamos que hubiera quedado más claro si se hubiese redactado en los siguientes términos: “Que dicho certificado haya sido emitido por un certificador licenciado conforme al art. 14 de esta ley, o reconocido según el art. 16”.

ART. 10 – Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

La norma regula la situación, nada infrecuente en el mundo moderno, de la contratación automática entre las computadoras. Obviamente el

---

de ser necesaria, evitando así que éstos puedan cometer errores en el momento de contratar”.

contrato no es entre las máquinas[30], sino que éstas han sido programadas expresamente para aceptar u ofrecer un determinado servicio comercial o profesional sin asistencia inmediata del operador; pero siempre el contrato es entre los sujetos que han preparado sus ordenadores para este sistema de contratación automática. Sobre todo el oferente, suele dejar programadas las operaciones de quienes requieran sus servicios. Así, el ordenador, ante el envío de una solicitud y previa verificación de la firma y validez del documento electrónico que contiene el mensaje de aceptación, lo que realiza de manera automática el ordenador, procede a validar la información y generar el vínculo negocial. Se trata en definitiva de una oferta que aguarda en el ciberespacio el instante mismo de la aceptación para generar el vínculo negocial. A pesar de lo moderno de la situación jurídica, el supuesto no escapa a la previsión de las normas del Código civil, que la regula acertadamente en los arts. 1144 y 1147.

Si se procuraba que la comunidad recepte positivamente este medio de contratación, obviamente el legislador debía generar un grado de certeza en la oferta automática; por ello se genera la presunción “iuris tamtun” de remisión por el oferente y su consecuente irrepudiabilidad. Pero si por cualquier circunstancia resultara que la oferta no era cierta, la carga de la prueba de dicha situación, recaerá sobre el autor de la oferta; mientras no lo haga la validez de la misma jugará en su contra.

Debe advertirse la audacia del legislador en este punto; pues mientras la firma holográfica, en la que tanto hemos confiado por muchos siglos, requiere para generar sus efectos vinculantes del reconocimiento expreso o presunto del firmante (arts. 1026 y 1028 del Código Civil), en materia de

[30] LUZ CLARA, Blanca; Ob. cit. Pág. 60. Llega a decir que estos ordenadores “(...) se independizan (...) respondiendo a un software previamente instalado, y que les permite tomar ciertas decisiones en el caso de ser necesario.” FARRÉS, Pablo; Ob.cit. pág. 128, expresamente aclara, explicando la Ley Modelo de la ONU, que “Ello no debe entenderse, sin embargo, en el sentido de que la Ley Modelo autorice la atribución de la titularidad de derechos y obligaciones a una Terminal informática.”

firma digital, todo lo contrario, la firma vale y vincula, aun remitida entre máquinas previamente programadas para hacerlo, desde el momento mismo de la recepción de la aceptación. Por ello habíamos establecido que el documento signado digitalmente ocupaba un lugar intermedio entre los instrumentos públicos y los privados (véase nuestro comentario al art. 7).

Nunca más adecuado referirnos en estos casos a los llamados “contratos de adhesión”; ya que, según el art. 1152 del Código Civil, si el aceptante modifica en algo la propuesta, deberá considerarse el nuevo envío como una nueva oferta de contratación, cuya decisión, obviamente escapa a la posibilidad de las máquinas.

ART. 11– Original. 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 y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

Esta norma es quizás la que más críticas nos merezca. En nuestra opinión no se ha tomado en cuenta la repercusión que puede tener el considerar originales a todos los que se han reproducido en formato digital (“bak up”) firmados a partir de originales de primera generación.

En primer lugar corresponde aclarar que cuando el legislador alude a originales de primera generación, se está refiriendo al original que fue elaborado por primera vez, si se nos permite la expresión aplicada al ámbito

informático, deberíamos decir que se refiere al primer ejemplar[31]. Es el que está conservado en el ordenador de quien confeccionó el texto documental. Pero, tal como habíamos adelantado, el considerar originales a todas las reproducciones que de él se hicieren, constituye un error conceptual en cuanto a las posibilidades de ejecución del mismo.

El hecho de considerarse original en el ámbito de la ley 25509, apunta a otra cuestión; se quiere con esta expresión hacer extensiva las garantías que la ley brinda a los originales, en cuanto a completividad, integridad, e inalterabilidad[32]. Pero no se ha advertido que la expresión usada, desde el punto de vista jurídico, se aplica al documento que genera la posibilidad de ejecutarse aun de una manera compulsiva; y, como las obligaciones contenidas en los documentos sólo pueden exigirse una sola vez, el documento debe perder eficacia, por cumplimiento, una vez prestado el servicio, entregada la cosa, etc.; es decir una vez cumplida la obligación instrumentada. Pero si los documentos son varios, esa primitiva y natural garantía, que constituye la enervación de eficacia del original, se ve seriamente perturbada, pues permanecerá intacta en el resto de los ejemplares “originales”.

Es curioso que especialistas en materia instrumental, no remarcaran este error conceptual de la ley bajo análisis y los problemas que puede acarrear el considerar a todas las copias como originales[33]. Esta circunstancia lejos de ser una ventaja del sistema, resulta todo un problema. Al deudor, una vez cumplida la obligación, no le bastará con eliminar o dejar sin efecto el contrato original, pues hay ya varios originales. Se trata de un problema de ejecutividad: El acreedor hipotecario, por ejemplo, debe presentar su título ejecutivo al juez para que proceda la ejecución, que una

[31] LUZ CLARA, Bibiana; Ob.cit., pág. 63.
[32] LUZ CLARA, Bibiana; Ob.cit. 63, 64. FARRÉS, Pablo; “Firma Digital”, Ob.cit. pág. 140 – 145.
[33] GATTARI, Carlos N.; “Manual de Derecho Notarial”, 2º Ed. Perrot, Bs.As. 2008, pág. 447.

vez cumplida eliminará la posibilidad de volver a accionar con ese documento. Al acreedor de un documento "pagaré" debidamente instrumentado, se le exigirá la presentación del original del instrumento respectivo, para que una vez logrado su fin (cumplimiento de la obligación) éste pierda definitivamente su ejecutividad.

En principio, todo lo que sea acción o disposición habrá de necesitar un título con valor ejecutivo. Así como nadie pagaría el monto correspondiente a un pagaré o un cheque sin que se le exhiba el documento y, además, se cuidará de anular su ejecutividad, no sólo mediante recibo, sino apoderándose del original, o quitándole la firma, o atestando su cumplimiento, tampoco nadie podría llegar a ejecutar un documento portante de un derecho cualquiera sin tener el título a la vista, y sin asegurarse de anular su ejecutividad[34] una vez utilizado. Téngase presente que cuando hablamos de "ejecutar" no siempre se hace referencia a una patología (cuando el derecho es desconocido por el deudor) sino que también corresponde aplicar el concepto de ejecución, al hecho de cobrarlo voluntariamente, sin necesidad de acudir a la Justicia; transferir el derecho documentado, modificarlo o ejercer cualquiera de las facultades que genere.

A ello se debe el celo del legislador civil, cuando rodea de exigencias el instrumento privado en cuanto al número de ejemplares y sus recaudos, en los arts. 1013, 1021 y 1024; así como las que requiere para la expedición de primeras y segundas copias en los arts. 1006 a 1008 del Código Civil[35].

A nuestro entender, el criterio del legislador al atribuir carácter de original a toda copia, constituye un error que transgrede el más elemental

---

[34] VENTURA, Gabriel B. "Algunos problemas vinculados a los testimonios y copias de escrituras", en Revista Notarial de Córdoba, Nro. 73, pág. 57.En el caso de los documentos portantes de derecho real, ello se logra con las notas marginales, en las que el notario consignará que el derecho se ha transmitido o se ha gravado con hipoteca, etc.

[35] FARRÉS, Pablo; Ob.cit. pág. 145 y ss. hace completa síntesis de las normas civiles relacionándolas con el artículo comentado.

principio de seguridad en la ejecución de los derechos; pero, al mismo tiempo, estimamos que no ha podido evitarse, dado que no creemos que sea factible determinar la procedencia (original o copia) mediante recursos informáticos[36].

El decreto reglamentario 2628/2002, determina en el art. 4, que será la Jefatura de Gabinete de Ministros la encargada de establecer las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico.

ART. 12 – Conservación. La exigencia legal de conservar documentos, registros o datos, también quedará satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

Esta norma aparece por demás lógica y consecuente con todo lo que venimos exponiendo; pues si el sistema torna válido el documento que exige firma ológrafa, cuando se lo ha firmado digitalmente, resulta de una coherencia incuestionable que también permita que los mismos archivos queden integrados por tales elementos digitales, así como la conservación de documentos que exijan las leyes, quede satisfecha mediante el archivo de esos instrumentos digitales, suscriptos también digitalmente.

De nuestra parte resulta más que claro que el dispositivo, al usar el adverbio “también”, procura “enganchar” si se nos permite la metáfora, tal

[36] VENTURA, Gabriel B. “Firma Digital”, LL, 2004 -B, 1274.

como lo hemos expresado en el párrafo precedente, el archivo digital, con el postulado fundamental de la ley, que pretende considerar satisfecha la necesidad de firma, cuando una norma lo solicita, mediante la firma digital, según lo sentado en la norma del art. 3 de la ley 25506. Sin embargo este artículo 12, ha sido criticado por Farrés, quien entiende que al haber empleado la expresión "también queda satisfecha", amén de no hacer aplicación del principio de no discriminación hacia las formas electrónicas que deben guardar las normas respecto de los documentos electrónicos, posibilita que erróneamente se vincule el dispositivo con documentos obtenidos por otros sistemas, como el escaneo de instrumento papel, del que surgirá su representación informática[37].

La necesidad de conservación, por otra parte, es recaudo elemental del derecho común. Recibos, reconocimientos de toda índole, registros y archivos laborales, declaraciones impositivas y contratos en general, no sólo requieren de su generación, sino que deberán ser esgrimidos en el momento oportuno, sea para ejercer compulsivamente un derecho, sea para acreditar el cumplimiento de recaudos administrativos formales.

En este sentido es innegable el aporte de la ley a la economía de tiempo y espacio. Hoy el soporte papel, aunque de nuestra parte lo consideramos el menos riesgoso jurídicamente hablando, constituye todo un desafío, por su peso, dificultades de acceso, deterioro por la manipulación y las dificultades de mantenimiento en buen estado en lugares que a veces no cuentan con los recaudos mínimos de temperatura, ventilación, etc.; pero, sobre todo por el lugar que ocupa[38]. Por algo, ya desde la década del setenta comenzaron a aparecer las técnicas de microfilmado para aliviar los

[37] FARRÉS, Pablo; Ob.cit. pág. 158, 159.
[38] LUZ CLARA, Bibiana; Ob.cit. pág. 66, 67, dice: "Por otro lado, el estado de conservación de dicha papelería en algunos casos se encuentra en estado lamentable, sufriendo las consecuencias de una deficiente conservación por la existencia de humedad, lugares sin ventilación y en muchos casos la existencia de roedores.

archivos de cargas y espacio. Pues bien, la posibilidad de almacenar y archivar, de manera válida y oficialmente reconocida por la ley, documentos digitales, aporta una solución a esos requerimientos.

Otro punto ventajoso de un archivo de documentos digitales, es la posibilidad de acceder rápidamente al elemento requerido, merced a la búsqueda informática que, en segundos, encuentra el documento solicitado.

CAPÍTULO II

De los certificados digitales

ART. 13 – Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

Esta norma presupone la existencia del llamado "Certificador licenciado" regulado a partir del art. 17 de la ley 25506, que es creado justamente para cumplir la función de firmar digitalmente los certificados mencionados en el artículo que analizamos.

El certificador analiza el documento remitido, firmado digitalmente por el emisor, y verifica fundamentalmente su procedencia merced a la clave pública del mismo[39]. Recordemos que este sistema, según vimos en nuestro análisis introductorio, trabaja con un procedimiento de criptografía asimétrica; es decir con la asignación de dos claves, una pública y otra privada.

[39] LUZ CLARA, Bibiana; Ob.cit. Pág. 72.

La clave pública se da a conocer por el usuario interesado en recibir información segura. La clave privada en cambio queda sólo en su poder cuidadosamente tutelada; dado que su divulgación hace peligrar la privacidad y seguridad de sus recepciones y envíos[40]. En definitiva requiere el cuidado que exigen los sellos de seguridad y los formularios oficiales personalizados, pues su extravío elimina uno de los recaudos que brindan seguridad al sistema.

Utilizando la clave pública del remitente cualquiera puede desencriptar su envío, que fue previamente encriptado mediante la clave privada del firmante. Lo encriptado con la clave privada pueda desencriptarse mediante la utilización de la clave pública e, inversamente, lo encriptado en la clave pública del receptor, pueda desencriptarse mediante su clave privada.

Ya habíamos expresado también que nada de esto podría lograrse sin la existencia de un intermediario en las comunicaciones, cuya misión es justamente verificar la autenticidad del envío. Toda remisión pasa previamente por una autoridad imparcial que es el certificante mencionado en el artículo 17 de la ley 25506, que tiene justamente la función de dar fe de la utilización de la clave privada del remitente y del destinatario. Remitimos para mayor comprensión de este artículo a lo expresado en relación al artículo 17.

El certificador licenciado emite el certificado digital, lo que acredita que los datos contenidos en un documento digital (art. 6) corresponden o son de autoría del firmante, así como su integridad y no alteración. Este

[40] VENTURA, Gabriel B.; "Firma digital y documento notarial", LL, 2004 -B, 1274. Decíamos ahí, criticando el sistema que "La firma sólo puede ser estampada por el titular, quien sólo mediante una situación de violencia compulsiva (vis relativa) podrá verse en la necesidad de estamparla involuntariamente. En cambio la digital puede llegar a conocimiento de terceros, sea por descuido, sea por manejo de la misma PC. en la que se encuentra grabada la firma digital. Todo operador de esa computadora podrá acceder a la firma. Será posible también la obtención de la firma digital mediante la violencia física o moral lográndose así una firma con todos los requisitos de autenticidad para el sistema digital".

certificado viaja adosado informáticamente al documento digital, y ambos documentos (el documento digital y su correspondiente certificado digital) son recibidos por el receptor.

Reafirmando lo dicho, el decreto reglamentario, en el art. 3, se refiere al certificado digital como "(...) aquellos cuya utilización permite disponer de una firma digital amparada por las presunciones de autoría e integridad establecidos en los artículos 7º y 8º de la ley citada".

ART. 14 – Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:

a) Ser emitidos por un certificador licenciado por el ente licenciante.

b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permiten:

1. **Identificar indubitablemente a su titular y al certificado licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;**
2. **Ser susceptible de verificación respecto de su estado de revocación;**
3. **Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;**
4. **Contemplar la información necesaria para la verificación de la firma;**
5. **Identificar la política de certificación bajo la cual fue emitido.**

Se enumeran en el dispositivo los recaudos necesarios para que el certificado sea válido y en consecuencia genere todos los efectos jurídicos que la ley le atribuye a la firma digital.

Analicemos los dos incisos por separado:

En el inciso a, exige que el certificado haya sido emitido por un "certificador licenciado", para lo cual hay que acudir a la definición que nos brinda el art. 17 de la misma ley: "Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante".

Cuando la ley exige que se trate de un certificador licenciado, tal como surge de la definición legal, requiere que esa licencia haya sido otorgada por el Ente Licenciante que, previamente a su otorgamiento, exigirá al solicitante de la licencia el cumplimiento de las condiciones exigidas en el art. 24 del Decreto Reglamentario 2628/02.

El sistema, en definitiva, deposita su confianza en este Certificador, tal como habíamos adelantado en nuestro análisis al art. 1. Nada podría lograrse sin la existencia de este intermediario en las comunicaciones, cuya misión es justamente verificar informáticamente la autenticidad de cada envío. El Certificador licenciado es el tercero de confianza que tiene la misión dar fe de la utilización de la clave privada del remitente y del destinatario. Responde de manera directa por su praxis[41].

A pesar de todas las exigencias requeridas por el Ente Licenciante al Certificador para otorgarle la licencia, la responsabilidad del Ente sólo se

[41] LUZ CLARA, Bibiana; Ob.cit. pág. 73. SALEME MURAD, Marcelo A.; "Firma Digital. Ley 25506 y Normativa Vigente", Ed. Ad-Hoc, Bs.As. 2004, pág. 23.

reduce al cumplimiento, por parte del licenciatario, de dichos recaudos, pues el licenciamiento no significará que se garantice el servicio ni los productos prestados por el Certificador; hay una expresa liberación de responsabilidad al respecto, en el Decreto Reglamentario, art. 25.

La definición legal del art. 17 de la ley 25506 resulta reproducida en su integridad en el glosario anexo al decreto reglamentario 2628/02, punto 5.

En el inciso b se exige que el certificado cumpla con los "formatos estándares" reconocidos internacionalmente. Si la finalidad del sistema de firma digital es lograr una contratación a distancia con cierta seguridad y garantía, para que se generen así todos los efectos jurídicos de la firma en general, es necesario que existan parámetros similares en todos los países. Ese es el motivo por el que se exige el "reconocimiento internacional" al que alude la norma.

La autoridad encargada de determinar qué estándares reconocidos internacionalmente se usarán a los fines de la ley 25506, es la Jefatura de Gabinete de Ministros, según lo expresa el art. 6, inciso a) del Decreto 2628/02: "Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer: a) Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales. (...)".

Son varios los estándares reconocidos; pero se ha determinado el empleo del estándar "X.509" en su versión 3[42]. Este formato estándar tiene la función informática de enlazar o vincular la clave pública con los datos que permiten identificar al titular de la misma.

En los puntos adicionados al inciso b, se agregan que el certificado debe identificar de manera indubitada al titular y también al certificador que lo emitió. Igualmente debe permitir verificar el estado del certificado mismo,

[42] FARRÉS, Pablo; Ob.cit., pág. 175. LUZ CLARA, Bibiana; Ob.cit. pág. 74.

en cuanto a que no haya sido revocado, conforme a lo dispuesto en el art. 23 del Decreto 2628/02.

Debe contemplar los datos necesarios para la verificación de la autenticidad de la firma, pues es la esencia del sistema. Con estos datos resultará de manera indubitada que la firma pertenece realmente al supuesto suscriptor y que el documento no ha sido alterado. Merced a la acreditación de estas circunstancias, una vez aceptada, aparece el efecto vinculante de la firma en los términos contractuales suscriptos.

En cuanto a la política de certificación a la que alude el último punto de la norma analizada, esta expresión está definida en el punto 6 del glosario del Anexo I del Decreto Reglamentario 2628/02, en los siguientes términos: *"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)".*

ART. 15 – Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.

La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

Dos causales de invalidez del certificado se encuentran siempre latentes: su caducidad y su revocación.

La caducidad opera una vez transcurrido el plazo por el que se ha otorgado el certificado, que como vimos debe contener la fecha de inicio y la fecha de su finalización. El solo transcurso del tiempo determina su invalidez y si se lo utiliza una vez producida su caducidad la firma carecerá de eficacia. Por ello es menester que resulte fácilmente accesible el dato del período de vigencia del mismo certificado.

Ocurre que una vez pasado cierto tiempo las claves podrían volverse vulnerables al permitir que algún operador, ajeno al vínculo negocial, pudiera desencriptar el contenido documental de los envíos, con el consiguiente daño al sistema[43]. Entre estos ataques que sufren las claves están los denominados "ataques de fuerza bruta" que consiste en dejar que el ordenador efectúe todas las numerosas pruebas posibles hasta encontrar la clave, aprovechando la gran capacidad de los procesadores modernos[44]. En algún momento la clave puede llegar a obtenerse y esto bastaría para restar credibilidad y seguridad al sistema de encriptación. Pero este ataque, por más sofisticados que fueren los elementos del agresor, nunca podrían producirse en el breve tiempo de validez de un certificado.

La revocación, en cambio, opera, según el artículo 19 que regula las funciones del Certificador Licenciado, en los siguientes casos: a solicitud del titular del certificado digital fuere cual fuere el motivo; como consecuencia de haberse detectado que fue emitido en base a una información falsa; si se

[43] SALEME MURAD, Marcelo; "Firma Digital. Ley 25506 y Normativa Vigente", Ed. Ad-Hoc, Bs.As. 2004, pág. 28. dice: "(...) mientras más tiempo posea un usuario un certificado digital, más vulnerable será. Por esa razón se ha entendido que no es conveniente que los certificados de firma digital tengan una vigencia de más de uno o dos años".
[44] LUZ CLARA, Bibiana; Ob.cit. pág. 75.

advierte que los procedimientos de emisión o de verificación han dejado de ser seguros; por cumplimiento de alguna de las condiciones establecidas en la política de certificación que lo rige; o, finalmente por resolución judicial o administrativa de la Autoridad de Aplicación. Este artículo 19 está reglamentado en el art. 23 del Decreto 2628/02 y se agregan allí algunas otras causales, como el fallecimiento del titular, declaración judicial de ausencia con presunción de fallecimiento del titular, cese de la relación de representación respecto de una persona, etc.

Se enumeran, en el artículo que analizamos, los recaudos necesarios para que el certificado sea válido y en consecuencia genere todos los efectos jurídicos que la ley atribuye a la firma digital.

En el segundo párrafo del artículo 15 se exige que el certificado tenga su vigencia dentro del lapso en el que la tenga a su vez el certificado digital del Certificador Licenciado. La lógica impera en este requerimiento, puesto que de no tener eficacia el certificado del Certificador surge obvio que no podría tenerla el certificado que éste hubiere emitido. Por eso entre los contenidos obligatorios del certificado, según expresa el artículo 14 y reitera el 15, está la fecha de inicio y finalización de su validez.

ART. 16 – Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o

b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

La gran utilidad que aporta el sistema de firma digital, lo determina la posibilidad de contratar a distancia mediante procedimientos que garanticen la autenticidad del envío, su integridad y autoría. Por ello tanto celo ha puesto el legislador en exigir recaudos técnicos y legales de verificación de los procedimientos regulados. Sólo mediante la utilización rigurosa de los sistemas reglamentados se podrán aplicar a la firma digital los típicos efectos jurídicos de vinculación negocial, sin riesgo para la seguridad jurídica. Pues bien, de poco serviría el sistema, o por lo menos se acotaría considerablemente, si sólo pudiera ser usado en el ámbito de un país determinado.

En este sentido se puede decir que la firma digital tiene vocación sinfrónica, muy propia, por otra parte, de los efectos de la globalización o mundialización que estamos viviendo en estos tiempos. Por ello se hace menester lograr que el sistema trascienda las fronteras del país y logre su cometido también respecto de otras naciones, posibilitando la contratación entre personas de distintos países. Tal como ocurre con todas las ramas del derecho privado, el tema es objeto del Derecho Internacional Privado, obviamente adaptado a toda la tecnología que demanda la firma digital.

Pues bien la ley 25506, en el artículo que analizamos, propone la posibilidad de considerar válido el certificado extranjero siempre que existan pactos de reciprocidad entre el país de origen y el nuestro, y que, tanto el certificado ajeno al nacional, como su certificador, cuenten con los mismos

recaudos que se le exigen al nacional, según los artículos que ya hemos comentado.

Por ello, y para facilitar la aplicación de la firma digital también respecto de certificados emitidos en el extranjeros se faculta especialmente a la Autoridad de Aplicación, la Jefatura de Gabinete de Ministros, a elaborar y suscribir acuerdos de reciprocidad con gobiernos de países extranjeros, según lo establece el Decreto Reglamentario 2628/02 en su artículo 28. Pero a los fines de evitar que este reconocimiento implique el desempleo de certificados argentinos, el mismo art. 28 del Decreto Reglamentario, en su parte final, determina que los certificados extranjeros no podrán ser empleados para la suscripción digital de documentos emitidos por personas residentes en la República Argentina.

El Decreto reglamentario, 2628/02 se refiere también a la validez al certificado emitido por un certificador extranjero en el art. 1 inciso d), en el que se reconoce como sistema de comprobación de autoría e integridad de la firma digital la *"(...) basada en certificados emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos: 1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero (...)"*.

CAPITULO III

Del certificador licenciado

ART. 17 – Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros

servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos.

El sistema, deposita su confianza en el Certificador Licenciado, tal como habíamos adelantado en nuestro análisis al art. 1 y 14. Nada podría lograrse sin la existencia de este intermediario en las comunicaciones, cuya misión es justamente verificar informáticamente la autenticidad de cada envío. El Certificador licenciado es el tercero de confianza que tiene la misión dar fe de la utilización de la clave privada del remitente y del destinatario. Responde de manera directa por su praxis[45]. Obviamente nos estamos refiriendo a la responsabilidad resarcitoria civil, puesto que, desde el punto de vista administrativo, la responsabilidad obligará a aplicarle las sanciones previstas en el artículo 41 de la ley 25506, previa instrucción sumaria que deberá llevar a cabo el Ente Licenciante, conforme a la Ley de Procedimiento Administrativo 19549 y su reglamentación (artículo 40, ley 25506).

Las sanciones son analizadas en nuestro comentario al art. 41, por ello para no incurrir en repeticiones nos remitimos a ese punto de nuestro trabajo.

El Ente Licenciante no responde por la conducta del Certificador, mientras haya corroborado adecuadamente el cumplimiento de todos los

[45] LUZ CLARA, Bibiana; Ob.cit. pág. 73. SALEME MURAD, Marcelo A.; "Firma Digital. Ley 25506 y Normativa Vigente", Ed. Ad-Hoc, Bs.As. 2004, pág. 23.

recaudos que la ley exige en la persona del Certificador. El licenciamiento no significa que se garantice el servicio ni los productos prestados por el Certificador. A tales fines se lo libera expresamente de responsabilidad al respecto, en el Decreto Reglamentario, art. 25.

Conforme a las tendencias actuales, la última parte del artículo que comentamos, expresa que los certificadores que no integren la administración pública quedarán sometidos a las reglas del mercado, en libre competencia.

ART. 18 – Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

En este artículo hay una apertura especial hacia los Colegios o Consejos Profesionales que nuclean ciertos sectores de actividad social. Es de destacar que si bien se admite que los Colegios o Centros, según los casos, cuenten con la posibilidad de usar firma digital y revestir la calidad de certificador licenciante, esto no significa que las citadas entidades utilicen esta licencia para brindar servicio a cualquiera. Por el contrario, su utilización debe estar ceñida a la función que la ley que las crea, les haya atribuido como administradores de la matrícula profesional y todo lo que resulte anexo a ese objetivo. Estimamos que este alcance acotado de aplicación resulta de manera bastante clara de la expresión usada en el dispositivo *“(...) podrán emitir certificados digitales en lo referido a esta función, (…)”*.

El presente artículo nos permite distinguir dos tipos de entidades certificantes o certificadoras: las abiertas y las cerradas. Mientras las primeras utilizan el servicio de certificación licenciada como fin primordial de un emprendimiento comercial, dirigido a quien quiera usar sus prestaciones, las segundas en cambio, lo utilizan en provecho propio y sólo para el núcleo cerrado de una comunidad determinada (Colegios de Abogados con sus profesionales, Colegio de Ingenieros, etc.). Por ello Luz Clara dice, refiriéndose al artículo 18 que anotamos, que "Se trata aquí de una comunidad cerrada, donde la autoridad certificante y sus suscriptores conforman todos parte de una misma institución, en este caso colegio profesional"[46]

Lógicamente para que se reconozca a los Colegios Profesionales como Certificadores Licenciados será menester que éstos cumplan con todas las exigencias que la propia ley requiere a los certificadores en general.

ART. 19 – Funciones. El certificador licenciado tiene las siguientes funciones:

a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;

b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;

[46] LUZ CLARA, Bibiana; Ob.cit. pág. 83.

c) **Identificar inequívocamente los certificados digitales emitidos;**

d) **Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y su vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;**

e) **Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:**

1. **A solicitud del titular del certificado digital.**
2. **Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación;**
3. **Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.**
4. **Por condiciones especiales definidas en su política de certificación.**
5. **Por resolución judicial o de la autoridad de aplicación.**

f) **Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.**

Lo primero que advertimos de la lectura del artículo que estamos analizando, es que se refiere a las funciones como si resultaran diversas de las obligaciones que asume el Certificador. Por ello, en el art. 21, cuando se reglamentan las obligaciones parecieran repetirse algunas. Sin dudas el legislador no ha tenido muy en claro qué diferencia una función de una obligación. Quizás hubiera sido conveniente, aunque resultara muy extensa, reducir las dos normas a una, ya que a cada función corresponde el deber de cumplirla adecuadamente.

Las funciones del certificador están fundamentalmente dirigidas a brindar seguridad al sistema, que se ha erigido en una expresión técnica: “confianza digital”; por ello se ha consignado en la misma norma que alude a sus atribuciones, los motivos por los que debe revocarse el certificado.

El primer inciso se le obliga a “recibir una solicitud de emisión de certificado digital”. Estimamos que el artículo debió decir, en forma indeterminada, “recibir las solicitudes de emisión de certificados digitales”; pero, amén de ello, es evidente que la norma regula toda una obviedad, puesto que ya ha quedado explicado en los precedentes artículos, sobre todo en el 13 y el 17, que más que la función del certificador, la recepción de las solicitudes y la emisión consecuente de los certificados constituyen la razón misma de su existencia. El sistema legal de firma digital descansa en el certificador por ser el tercero de confianza que un sistema de criptografía asimétrica, como el previsto en la ley 25506 exige. El recibe la solicitud, como expresáramos y expide el consecuente certificado.

En esta actividad debe respetar las reglamentaciones e instrucciones de la Autoridad de Aplicación y las políticas de certificación que previamente se hayan acordado, conforme lo previsto en la reglamentación. Recordemos que las políticas de certificación a las que alude la norma, están referidas a

los 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, conforme lo conceptualiza el “glosario” final contenido en el Decreto Reglamentario 2628/02. Estas políticas de certificación, cuyo contenido mínimo está previsto en el art. 29 del citado decreto, integran el contenido de una suerte de contrato por adhesión, al que han quedado vinculadas las partes: el certificador y el usuario.

En cuanto a la exigencia de identificar inequívocamente los certificados digitales emitidos, la norma se refiere a la necesidad de desplegar toda la capacidad informática para determinar la identidad e integridad del certificado que irá acompañando al documento motivo de la contratación o declaración; puesto que es la finalidad primordial de la ley el garantizar estos requisitos en los envíos. Constituyen en realidad la aplicación de recursos técnicos, más que conocimientos en particular; pero tienen también una importante dosis de criterio humano en cuanto a las dudas e inseguridades que puedan plantearse. Estas pueden llegar hasta a llevarle a decidir la revocación de un certificado, conforme a lo establecido en la misma norma, inciso e, puntos 2 y 3.

El certificador debe mantener un archivo informático de todas las solicitudes de certificados y los certificados mismos que se hayan emitido, obviamente en condiciones de inalterabilidad, puesta que la función del mismo es tutelar el sistema permitiendo rehacer la prueba de los mismos. Por ello este archivo debe posibilitar acceder a su contenido de manera cierta . Recordemos que la misma ley 25506, prevé la posibilidad de guardar la documentación en archivos informáticos conforme lo establecido en el art. 12.

Habíamos dicho que la necesidad de conservación, es un recaudo elemental del derecho común. Recibos, reconocimientos de toda índole, registros y archivos laborales, declaraciones impositivas y contratos en

general, no sólo requieren de su generación, sino que deberán ser esgrimidos en el momento oportuno, sea para ejercer compulsivamente un derecho, sea para acreditar el cumplimiento de recaudos administrativos formales. Pues bien, esa es la función que asigna la ley 25506 al archivo informático de los certificadores licenciados.

En cuanto a la revocación de certificados que la ley atribuye como función al certificador licenciado, ya nos hemos referido a esta circunstancia, en oportunidad de anotar el art. 15. La revocación opera en los siguientes casos: a solicitud del titular del certificado digital fuere cual fuere el motivo; la que podrá formalizarse por escrito, mediante soporte papel o mediante remisión informática a través de la red, con suscripción digital; como consecuencia de haberse detectado que fue emitido en base a una información falsa; si se advierte que los procedimientos de emisión o de verificación han dejado de ser seguros; por cumplimiento de alguna de las condiciones establecidas en la política de certificación que lo rige; o, finalmente por resolución judicial o administrativa de la Autoridad de Aplicación.

Este artículo 19 está reglamentado en el art. 23 del Decreto 2628/02 y se agregan allí otras causales: por fallecimiento del titular; por declaración judicial de ausencia con presunción de fallecimiento del titular (arts. 22 y 23 de la ley 14394); por declaración judicial de incapacidad del titular; si se determina que la información contenida en el certificado ha dejado de ser válida y por el cese de la relación de representación respecto de una persona.

También existe la obligación de informar del certificador, tanto respecto de los certificados emitidos, como los que hayan sido revocados. Para ello se confeccionan listas especiales, a las que tienen acceso los usuarios ante simples solicitudes. En algunos artículos del decreto reglamentario se ajustan o precisas estas informaciones, a la par que se

agregan otros deberes de información. Por Ej. el artículo 34 inciso g, expresamente determina que entre las obligaciones del certificador licenciado está la de “Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados”. Igualmente en el inc. h) “Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador”. En el inc. o) “Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada”. En el inc. q) “Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él”.

ART. 20 – Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

La norma cuyo análisis abordamos sólo expresa que quien pretenda ser certificador licenciado deberá solicitar la licencia y cumplir con todas las exigencias personales y técnicas que surgen de la reglamentación. La que determina cuáles son esos recaudos es el artículo 24 del Decreto Reglamentario 2628/02, que pasará a ser así la verdadera norma analizada.

Dice el art. 24 de la reglamentación que *“Para obtener una licencia, los proveedores de servicios de certificación deberán particularizar las actividades para las cuales requieren la licencia y acreditar por los medios que este determine ante el Ente Administrador de Firma Digital: a) Documentación que demuestre: 1- En el caso de personas jurídicas su personería. 2- En el caso de registro público de contratos, tal condición. 3-*

En el caso de organización pública, la autorización de su máxima autoridad para iniciar el proceso de licenciamiento y la correspondiente aprobación de la JEFATURA DE GABINETE DE MINISTROS, de acuerdo con lo dispuesto en el artículo 41 de la presente reglamentación. b) El cumplimiento de las condiciones establecidas en la ley; este decreto y las normas complementarias. c) Las políticas de certificación para las cuales solicita licencia que respaldan la emisión de sus certificados. Manual de Procedimientos, Plan de Seguridad, Plan de Cese de Actividades y Plan de Contingencia satisfactorias de acuerdo con las normas reglamentarias. d) Toda aquella información o requerimiento, que demande la Autoridad de Aplicación.

La primera exigencia que aparece en esta norma, es la determinación de las actividades para las cuales se requiere la licencia. La solicitud deberá expresar, por ejemplo, si se tratará de un sistema abierto o cerrado, si será la única actividad de la empresa la prestación de servicio de certificación de firma digital, etc.

Si la peticionante fuera persona jurídica, deberá agregarse al expediente de solicitud, la documentación que acredite la personería; es decir el contrato social debidamente inscripto en el Registro pertinente, estatutos, las actas de distribución y designación de cargos, en su caso; las actas que acrediten la toma de la decisión social, etc. y todo lo que legalmente corresponda, según el tipo social de que se trate, para considerar válida la voluntad social de solicitar la licencia.

De ser un Registro Público de contratos, deberá acompañarse igualmente la acreditación de la condición de tal, y de la representación que invoque el peticionante. Si el registro es una organización pública, dependiente de la administración, deberá requerirse también la autorización de la superioridad para incorporarse al sistema.

Si se trata de organizaciones públicas nacionales, se exigirá además la correspondiente aprobación de la Jefatura de Gabinete de Ministros (art. 41 de la reglamentación). Destacamos que se refiere sólo a los casos en que la Organización Pública fuere del orden Nacional; ya que en este aspecto, la reglamentación sólo podría tener alcance Nacional; y es, por otra parte, lo que surge del referido artículo 41, que expresamente alude a las entidades y jurisdicciones de la Administración Pública Nacional.

Las previsiones de los incisos siguientes, procuran que la Entidad Licenciante tenga un cierto grado de certeza de la capacidad operativa del solicitante de la licencia. Recordemos que si bien la responsabilidad frente al usuario es directa del certificador licenciado, puede derivar al Ente lienciante si no puso el celo adecuado en requerir y verificar luego, mediante auditorías e inspecciones, la existencia y cumplimiento de tales exigencias que constituyen, al mismo tiempo, una garantía práctica de viabilidad.

En el punto c) del art. 24 de la reglamentación, se exigen varias previsiones al solicitante que determinarán cómo y en qué condiciones está dispuesto a prestar el servicio de firma digital. Por ello, con expresiones técnicas acotadas en cuanto a su sentido y alcance, la norma requiere que el peticionante presente el “Manual de Procedimientos”, que se refiere al conjunto de prácticas utilizadas por el certificador licenciado en la remisión y administración de los certificados, para que el usuario sepa a qué atenerse ante cada situación que se pueda presentar en el servicio de certificación de firma digital que prestará el certificador licenciado.

Con la exigencia de presentación del Plan de Seguridad, se le está requiriendo la previsión de las prácticas y procedimientos que se utilizarán en la prestación del servicio destinado a la protección de la información: confidencialidad, autoría, privacidad de las claves, etc. En cuanto al Plan de Cese de Actividades, mencionado también por la norma del 24, se refiere a la forma en que se efectivizará el corte de actividades del certificador

licenciado; lo que involucra entrega de documentaciones y archivos, notificaciones, etc. Finalmente, se le exige al peticionante que presente el Plan de Contingencia, que vendría a ser algo así como la previsión de lo imprevisto, si se nos permite la paradoja; y consiste en conocer de antemano qué hará el certificador licenciado en caso de ocurrir situaciones no previstas que comprometan la continuidad de sus servicios.

Todos estos planes deberán sortear un minucioso análisis del Ente Licenciante en el expediente de solicitud que concluye con un dictamen legal y técnico. En caso de no satisfacerse los requerimientos, el trámite será observado.

Como se puede advertir, en todos estos requerimientos se procura como fin primero y último, brindar seguridad, ya que sin este objetivo cumplido, el sistema no se utilizará y ningún usuario arriesgará sus emprendimientos contratando mediante la firma digital.

En el glosario final del Decreto 2628/02 se define con cierta precisión cada una de las expresiones usadas en su art. 24.

ART. 21 – Obligaciones. Son obligaciones del certificador licenciado:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible.

La parte pertinente de dicha información estará también disponible para terceros;

b) 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 él emitidos;

c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;

d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;

f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

g) Mantener la confidencialidad de toda información que no figure en el certificado digital;

h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;

i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;

k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;

l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;

m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;

o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;

p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;

q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;

r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;

s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;

t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;

u) Constituir domicilio legal en la República Argentina;

v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;

w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante

Como habíamos adelantado al anotar el artículo 19 de esta ley, se mezclaban en cierta forma, las funciones del certificador con sus obligaciones y hasta con las correlativas responsabilidades frente al incumplimiento, según lo sentado en la ley, a partir del artículo 40.

En la norma cuyo análisis abordamos, bajo el título de obligaciones del certificador licenciado, se especifican las actividades que deben desplegar los certificadores licenciados; pero evidentemente no se ha tenido en cuenta ningún criterio de clasificación para enumerar las obligaciones, lo que dificulta en grado sumo su correcta asimilación y posibilita la omisión de algunos deberes.

Tenemos determinado que las obligaciones que asume cualquier agente público, pueden clasificarse en dos grupos: Las obligaciones generales, que podrían también denominarse estructurales, dado que hacen a los recursos técnicos y documentales que posibilitan al Certificador ingresar al sistema y que no se ponen de manifiesto en cada prestación del servicio, sino que están latentes puesto que son previas al ejercicio de su función; y las obligaciones particulares, que son las que se ponen de manifiesto en cada prestación de servicio.

Las obligaciones generales se caracterizan porque no aparecen en ellas los destinatarios directos del sistema, que serían los firmantes de la documentación digital. Se trata del cumplimiento de los recaudos básicos para ingresar a ser certificadores licenciados. Así, podemos mencionar entre ellas todas las que surgen del artículo 24 del decreto reglamentario, 2628/02: acreditar el cumplimiento de las condiciones establecidas en la ley; tener especificadas las políticas de certificación para las cuales solicita licencia que respaldan la emisión de sus certificados; tener previsto el Manual de Procedimientos y el Plan de Seguridad; el Plan de Cese de Actividades y el Plan de Contingencia satisfactorias de acuerdo con las normas reglamentarias; así como toda otra información o requerimiento, que demande la Autoridad de Aplicación. Igualmente sería una obligación general la establecida en el inciso c de la norma que analizamos; es decir “mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación”. También el inciso d que establece que el

certificador debe operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación. El inciso j también prevé una obligación general cuando exige que el Certificador debe incorporar en su política de certificación los efectos de la revocación de su propio certificado digital o de la licencia que le otorgara a autoridad de aplicación.

También serían obligaciones generales, las establecidas en los incisos q, r, s, t, u, y v, que le exigen informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia; permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo para poner a su disposición toda la información necesaria y brindarles la asistencia que sea menester; emplear personal idóneo con el conocimiento y la preparación suficientes para la prestación del servicio; someter a aprobación del ente licenciante el manual de procedimientos, el plano de seguridad y el de cese de actividades así como el detalle de los componentes técnicos a utilizar; constituir domicilio en la República Argentina. Como habíamos adelantado al analizar el artículo 20, todos estos planes deberán sortear un minucioso análisis del Ente Licenciante en el expediente de solicitud que concluye con un dictamen legal y técnico. En caso de no satisfacerse los requerimientos, el trámite será observado. Pero, reiteramos, éstas obligaciones son previas al inicio de las actividades o por lo menos son de tipo estructurales para poder cumplirlas.

Como obligaciones particulares o singulares, podemos mencionar las que aparecen en los incisos a, b, e, f, g, h, i, k, m, n, o, p y w. Así, deberá informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su

posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorgara el ente licenciante; abstenerse de tomar conocimiento o acceder bajo ninguna circunstancia a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos; notificar el solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable , y las obligaciones que asume por el solo hecho de ser titular de un certificado digital; solicitar sólo los datos necesarios para emitir el certificado digital, informándolo de todo lo que se refiere a su tramitación; mantener la confidencialidad de la información que no figure en el certificado digital; mantener la documentación respaldatoria de los certificados digitales emitidos, por diez años a partir de su fecha de vencimiento o revocación; publicar la lista de certificados digitales revocados y el resultado de los informes de la última auditoría que se le haya efectuado, conforme al artículo 27, 33 y 34 de la ley 25506; registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas; informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular; verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales; solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros y cumplir con toda otra obligación emergentes de su calidad de titular de la licencia adjudicada por el ente licenciante.

Corresponde destacar que, en todas estas obligaciones se encuentra presente también de manera genérica, la tutela que la ley 24240, prodiga a los consumidores en general, a partir de los artículos 7 al 10 bis. En

especial, en todo lo que se refiere a información[47], se aplicará la exigencia del idioma nacional, completividad, claridad, sin reenvíos a textos o documentos que no se entreguen previa o simultáneamente.

También tiene vinculación esta norma, tal como lo pone de resalto Luz Clara, con la ley 25326, de 2000, referida a la "Protección de los datos personales"[48]. Toda información a la que acceda el certificador licenciado, referido a las personas que usen el sistema de firma digital, queda sometida a la obligación de confidencialidad; y esta ley regula de manera pormenorizada, sobre todo en sus artículos 3 a 6, la protección y privacidad de tales datos.

En el decreto reglamentario 2628/02 se determinan otras obligaciones. Esta norma es pasible de las mismas críticas que le hemos efectuado a la norma del artículo 21 de la ley 25506; pero además corresponde destacar que resulta reiterativa, a pesar de expresar "además de lo previsto en el artículo 21 (...)". En efecto, dice el artículo 34 del decreto reglamentario que, *"Además de lo previsto en el artículo 21 de la Ley N° 25.506, los certificadores licenciados deberán:*

a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita.

b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.

---

[47] OSSOLA, Federico y VALLESPINOS, Gustavo; "La Obligación de Informar", Ed. Advocatus, Córdoba, 2001, pag. 137 y ss.
[48] LUZ CLARA, Bibiana; Ob.cit. pág. 91.

c) Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.

d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.

e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

f) Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.

g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

h) Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.

i) Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

j) Informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.

k) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.

l) Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;

m) Cumplir las normas y recaudos establecidos para la protección de datos personales.

n) En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley N° 25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.

El Ente Administrador deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital.

o) Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada.

p) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.

q) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él".

ART. 22 – Cese del certificador. El certificador licenciado cesa en tal calidad:

a) **Por decisión unilateral comunicada al ente licenciante;**

b) **Por cancelación de su personería jurídica;**

c) **Por cancelación de su licencia dispuesta por el ente licenciante.**

La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos.

El artículo cuyo análisis abordamos prevé el cese de la actividad del certificador licenciado, por las distintas causas enumeradas. El sistema regulado procura, como se advierte, reducir al mínimo los daños que se pudieren causar a terceros o usuarios en general.

Cuando se alude a la decisión unilateral se entiende que se refiere a la del Certificador, quien deberá comunicar tal circunstancia al Ente licenciante. No sería dable que el Ente Licenciante decida unilateralmente, revocar o hacer caducar la licencia del Certificador, pues que para que eso se haga procedente, se tienen que haber cumplido las condiciones para generar esa sanción, conforme a la previsión del artículo 44 y artículo 27 del Decreto Reglamentario, supuesto que está expresamente contemplado en el inciso c) de la norma analizada.

El certificador, una vez tomada la decisión, amén de comunicar la circunstancia al Ente Licenciante, debe cumplir todos los pasos y recaudos que él mismo ha asumido al formular sus Planes de Cese de Actividades y de Contingencias, regulados en el artículo 21 al que ya nos hemos referido y el artículo 24 del Decreto Reglamentario, que se refiere a la forma en que se efectivizará el corte de actividades del certificador licenciado; lo que involucra entrega de documentaciones y archivos, notificaciones, etc. Obviamente en caso de generarse daños por incumplimiento de las normas concretas que regulan el supuesto o de los planes preestablecidos, deberán

resarcirse los daños producidos conforme a las normas del Código Civil (artículos 506, 511, 512, 1077 y 1109 del Código Civil).

El segundo supuesto previsto en este artículo es el caso en que se produzca la cancelación de la personería jurídica del certificador por cualquier motivo que fuere; sea por expiración del plazo contractual, sea por decisión de los propios socios o por pérdida del capital social, etc.

Finalmente, como consecuencia de una sanción el Ente licenciante puede cancelar la licencia, tal como lo prevé el artículo 41, inciso c, que remite a la reglamentación y el artículo 44. El Decreto 2628/02 determina, en el artículo 27 que procederá la cancelación de la licencia en los siguientes casos: a) Falta de presentación de la declaración jurada anual; b) Falsedad de los datos contenidos en la declaración jurada anual; c) Dictamen desfavorable de auditoría basado en causales graves; d) Informe de la inspección dispuesta por el Ente Administrador desfavorable basado, en causales graves; y e) Cuando el certificador licenciado no permita la realización de auditorías o inspecciones dispuestas por el Ente Administrador.

No podemos dar por terminado nuestro análisis a este artículo 22, sin reprochar al legislador la falta de terminología técnica usada en casi todas estas normas que aluden a la caducidad; pues en ellas la expresión está utilizada más como cancelación que como caducidad misma. Si bien ambos institutos jurídicos (cancelación y caducidad) operan la ineficacia funcional de la licencia o del certificado, según los casos, las causas de la aplicación de uno u otro instituto son bien diferentes. Así, diremos que correspondería hablar de caducidad cuando un certificado pierde eficacia por el transcurso del tiempo; si se usa fuera de su período de validez, la firma no valdrá, según vimos al analizar el artículo 9 y 15 de la ley 25506; o cuando la licencia se hubiere concedido por un plazo determinado y éste ha transcurrido ya. En tales supuestos no sería menester ni siquiera un acto

solemne de cancelación, puesto que el solo vencimiento del plazo ya operó la ineficacia funciona; sus efectos son automáticos y requieren, obviamente, por parte del intérprete del certificado, el conocimiento adecuado para efectuar esa lectura

Para hablar de cancelación, en cambio, se exige una determinada acción por el Certificador o el Ente Licenciante. Así, por ejemplo, en todos los casos en que la ley habla de caducidad por aplicación de sanciones al certificador, en realidad se estaría aludiendo a situaciones que prevén cancelaciones. Por ello deben considerarse supuestos de cancelación los previstos en los artículos 41 inc. c). En el artículo 44, el error es aún más palpable ya que directamente la norma comienza mencionando la caducidad como una sanción: “Podrá aplicarse la sanción de caducidad de la licencia (...)”; cuando en realidad debería decir “Podrá aplicarse la sanción de cancelación de la licencia...”. Igualmente ocurre con el artículo 27 del Decreto Reglamentario 2628/02. Se aplica correctamente el término en el artículo 22 que comentamos que dispone que cesa el certificador en sus funciones “(...) por cancelación de su licencia dispuesta por el ente licenciante”.

Remarcamos algunos supuestos omitidos que, obviamente, también determinarán la caducidad de la licencia. Se trata de los supuestos de fallecimiento o incapacidad del certificador, correlato directo de la cancelación de la personería en las personas jurídicas, previsto en el inciso b) de la norma analizada.

ART. 23 – Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:

a) Para alguna finalidad diferente a los fines para los cuales fue extendido;

b) Para operaciones que superen el valor máximo autorizado cuando corresponda;

c) Una vez revocado.

Los supuestos previstos son la consecuencia de la previa calificación que debe efectuar el Certificador licenciado, recurriendo a los recursos tecnológicos con que cuenta, así como a las distintas políticas que ha asumido y los registros de recepción y emisión que debe llevar de manera segura.

Si complementamos este dispositivo con los artículos 14 y 15 de la ley advertimos que aquí el legislador ha puesto el acento en cuestiones más sustanciales, sobre todo en los incisos a y b. Dentro de las políticas de certificación pueden haberse especificado finalidades restrictas del uso de la firma digital por ese Certificador Licenciado, tal como puede ocurrir con las entidades que controlan la matrícula profesional de ciertas disciplinas (Colegios profesionales de abogados, escribanos, ingenieros, etc.); igualmente se aplicará esta norma cuando se utilice la firma digital para algún supuesto no permitido en forma genérica, en el artículo 4, por ejemplo suscribiendo una declaración sobre el reconocimiento de paternidad, o en un testamento.

Según la autorización otorgada por el Ente Licenciante, las atribuciones del Certificador podrán contener limitaciones, por cuestiones de seguridad, en cuanto a los valores en juego dentro de los contratos o declaraciones suscriptos con firma digital. Estas limitaciones surgirán de la resolución de licencia y, sin dudas, obedecerá al grado de solvencia acreditado y a su política de certificación y plan de contingencias propuesto. Tal sería la situación aludida en el inciso b de la norma comentada.

En cuanto al inciso c, no deja de ser repetición de lo ya establecido por la ley en el artículo 15, reglamentado en el artículo 23 del Decreto 2628/92. Remitimos a nuestro comentario al artículo 15 y 19 a los fines de completar los supuestos de revocación.

CAPITULO IV

Del titular de un certificado digital

ART. 24 – Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:

a) A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;

c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;

d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

e) A que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

Como todo contrato, el celebrado entre el Certificador Licenciado y el usuario que se hará titular del certificado, genera derechos y obligaciones. Se trata de un contrato con cláusulas predispuestas que está medianamente regulado en la ley que comentamos. Ya hemos expresado que el Certificador Licenciado debe solicitar su licencia y, previamente, debe presentar una serie de planes, determinados en el artículo 24 del Decreto Reglamentario 2628/02; pues bien, ellos están referidos a las políticas de certificación, manual de procedimientos, plan de seguridad, plan de cese de actividades y plan de contingencias; garantizar un sistema adecuado para mantener la confidencialidad de los datos y cualquier otro aspecto del usuario. Estos planes integrarán parte de las cláusulas predispuestas a las que habrá de someterse el certificador en el cumplimiento de su contrato. Como contrapartida, esas obligaciones del Certificador integrarán el cúmulo de derechos o facultades del titular del certificado, dado que él ha tenido en cuenta todas esas predisposiciones al momento de contratar; por ello el contenido de este dispositivo aparece como sobreabundante[49].

[49] FARRÉS, Pablo; Ob.cit. pág. 280, dice: "(...) la ley argentina trata un artículo inútil, puesto que todos los derechos que enumera son deducibles de las obligaciones del certificador".

Corresponde efectuar una crítica al texto mismo de la norma, pues en el primer inciso nos dice que el titular del certificado tiene el derecho a ser informado con carácter previo a la emisión del certificado, y agrega: “utilizando un medio de comunicación”. Realmente no existe otra posibilidad, si no es empleando un medio de comunicación, como pueda llegarle la información al titular del certificado. Seguramente la norma habrá querido decir un medio de comunicación fehaciente, o algo por el estilo, vinculado con la seguridad en dicha comunicación.

Dejando de lado esa dificultad interpretativa sobre un aspecto que, ciertamente no es esencial en el dispositivo, nos adentraremos ahora a los derechos que generaría el contrato mencionado al titular del certificado. Así, en cada inciso se mencionan las condiciones precisas de utilización del certificado. Recordemos que el certificado es el que “viaja” adosado informáticamente al documento digital, y ambos documentos (el documento digital y su correspondiente certificado digital) son recibidos por el receptor, garantizando así la autoría e inalterabilidad propia del sistema, y logrando por esto la irreprochabilidad del contenido y su natural efecto vinculante, una vez producida su aceptación por el co contratante.

Reafirmando lo dicho, el decreto reglamentario, en el art. 3, se refiere al certificado digital como “(...) aquellos cuya utilización permite disponer de una firma digital amparada por las presunciones de autoría e integridad establecidos en los artículos 7º y 8º de la ley citada”.

Fácilmente se advierte así que, dentro de la enumeración de las facultades del titular ha faltado el derecho fundamental, motivo de la implementación del sistema de firma digital, que es el derecho a “suscribir” la documentación de que se trate, mediante el certificado emitido y adherido al primero.

Tiene derecho también a que se le informe acerca de las características y efectos de dicho certificado, la existencia del sistema de licenciamiento y los procedimientos asociados. Toda esta información, cumpliendo con la ley 24240, artículo 4, debe ser brindada "…por escrito en un lenguaje fácilmente compresible".

Igualmente se le deberá informar de los costos que resultarán de la utilización del certificado, incluyendo cargos adicionales y formas de pago de los mismos; así como el domicilio en Argentina del Certificador y sobre los medios a los que podrá acudir el titular del certificado para solicitar aclaraciones o presentar reclamos y dar cuenta del mal funcionamiento del sistema.

Se le ha dado cabida especialmente, adelantándose a la posibilidad fáctica del Certificador, al derecho del titular del certificado a exigir que no se emita publicidad de ningún tipo a través del sistema de certificación digital. Evidentemente el hecho de estar regulada esta prerrogativa dentro de los derechos del titular del certificado, no obsta a que figure entre las cláusulas contractuales. La ley confiere ese derecho al titular, pero sólo a él. No coloca la prohibición entre los aspectos fundamentales del sistema, por lo que estimamos que, no alterándose el orden público, podría ser objeto de convención entre las partes negociales.

ART. 25 – Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;

c) Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

Como reza el proloquio latino “ius et obligatio sunt correlatio” (Derecho y obligación son correlativos), a todo derecho corresponde una obligación; en nuestro caso, nadie es más interesado en mantener la seguridad de su sistema de contratación que el destinatario directo; es decir el firmante. Por ello la ley le asigna, en la norma que comentamos, los deberes correlativos de confidencialidad e igualmente la utilización de un sistema de creación de firma digital confiable, puesto que si lo que falla es su sistema de creación de firma, no será dable reprochar la alteración o divulgación de su mensaje o clave al Certificador. Por ejemplo si mantiene en su ordenador la firma digital y su clave privada ya preconfigurada y alguien, sin su autorización, ingresa al mismo y suscribe digitalmente un documento que el titular no quería suscribir, la responsabilidad sería ahí del titular del certificado, pues él debía mantener el control exclusivo de sus datos de creación de firma digital, tal como le impone el art. 25, inciso a) de la ley 25506.

En realidad estas supuestas obligaciones del titular del certificado, más que obligaciones, son deberes, puesto que no corresponden al concepto técnico de obligación, sino al de deber jurídico. Aquí no hay un vínculo negocial, sino un deber correlativo de cooperación a la confidencialidad del sistema, cuyo principal interesado, como expresamos, es el firmante mismo.

En los otros incisos, se le impone al titular del certificado que, frente a la advertencia en cuanto a que pueda haberse comprometido la privacidad de sus datos de creación de firma, debe solicitar inmediatamente la revocación del certificado digital; igualmente debe informar sin demora al certificador, cuando advirtiera que han sido modificados algunos de los datos contenidos en el certificado verificado. La ley no pone plazos de notificación ni de solicitud de revocación, sólo se atiene a la lacónica expresión “sin demora”, dado que descansa en el interés primario y la única responsabilidad del destinatario final del sistema; es decir el usuario.

El incumplimiento de estos deberes, más que generarle responsabilidades al titular del certificado, libera de las mismas al certificador licenciado. Sólo podrá atribuírsele responsabilidad al titular si no cumpliere los deberes aquí asignados, cuando su omisión generare daños a terceros, pero no frente al certificador. Un ejemplo podría ser si, por ejemplo, no comunica al Certificador Licenciado que su clave privada ha sido divulgada y alguien, usando la misma, contrata con un tercero. La irreprochabilidad funcionará igualmente por no haber comunicado en tiempo y no podrá endilgar responsabilidad alguna al Certificador. Frente al tercero, el único responsable será el titular del certificado.

Distinto es el supuesto en que el titular es obligado por violencia, absoluta o relativa, a negociar mediante el certificado. Este tema ya no involucra el sistema de firma digital, y queda regulado con las normas del derecho común sobre los vicios de la voluntad[50]. La nulidad aquí se impone, luego de la investigación correspondiente, por existir un vicio en la contratación (art. 1045 C.C.). El supuesto equivale a forzar a la suscripción de una firma ológrafa a punta de pistola.

[50] LUZ CLARA, Bibiana; Ob. Cit. Pág. 102.

CAPITULO V

De la organización institucional

ARTÍCULO 26. — Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

ARTICULO 27. — Sistema de Auditoría. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

ARTICULO 28. — Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

En este capítulo, mediante las tres normas que analizamos, el legislador no hace más que repetir conceptos y regulaciones. Algunas cuestiones ya han sido tratadas en artículos anteriores, como lo previsto en el artículo 26; y otras serán objeto de análisis en normas posteriores; dado que hay un capítulo expreso dedicado a la Comisión Asesora y otro dedicado al sistema de auditoría[51].

[51] FARRÉS, Pablo; Ob.cit. pág. 300, dice: "(...) se trata de una vuelta atrás inútil, respecto del certificado emitido en el extranjero (de nuestra parte creemos que el legislador se quiso remitir al artículo 14 no al 16) (...), mientras que sobre los dos artículos restantes (27 y 28) lo innecesario será hacia delante (...)" (lo entre paréntesis es una aclaración nuestra).

El artículo 26 constituye una repetición de lo ya establecido como recaudo de validez de la firma digital, en el artículo 16, respecto de los certificados extranjeros; no se puede comprender el motivo de la reiteración del dispositivo. Ensayando una explicación diremos que quizás el legislador haya sentido la necesidad de brindar, con un criterio didáctico, las bases de la regulación del sistema: El Certificado Digital expedido por un Certificador Licenciado; El Sistema de Auditoría que evalúa la confiabilidad del Certificado Digital y finalmente la Comisión Asesora que, integrada por personal técnico informático, jurídico, administrativo y contable, permite conocer el grado de seguridad que brinda el sistema. Mediante estos tres "pilares" se construye el sistema de firma digital con cierto grado de seguridad.

Creemos que ese ha sido el criterio del legislador y, obviamente, siendo así, la remisión al artículo 16 ha sido un error. La norma a la que se ha querido aludir en el artículo 26 es la primera que refiere a los recaudos de validez de los certificados digitales; es decir el artículo 14.

En cuanto al artículo 27, se menciona allí lo que resulta imprescindible en un régimen que impone obligaciones estructurales: las auditorías; es decir el establecimiento de un sistema de inspecciones periódicas ordinarias o extraordinarias, para tomar conocimiento directo respecto al cumplimiento de las tales obligaciones. El tema se encuentra luego regulado en forma detallada en las normas de los artículos 33 y 34, en razón de lo cual remitimos a nuestro análisis sobre dichos dispositivos.

Otro tanto ocurre con el artículo 28, en el que se menciona por primera vez en la ley la Comisión Asesora para la infraestructura que, como veremos al analizar los artículos 35 y 36, se integra con profesionales de distintas disciplinas relacionadas con el sistema de firma digital. Remitimos a nuestro análisis de las citadas normas.

CAPITULO VI

De la autoridad de aplicación

ARTICULO 29. — Autoridad de Aplicación. La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

ARTICULO 30. — Funciones. La autoridad de aplicación tiene las siguientes funciones:

a) Dictar las normas reglamentarias y de aplicación de la presente;

b) Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;

c) Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;

d) Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;

e) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;

f) Actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;

g) Determinar los niveles de licenciamiento;

h) Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;

i) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;

j) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;

k) Aplicar las sanciones previstas en la presente ley.

Ya se había establecido que la autoridad de aplicación es la Jefatura de Gabinete de Ministros; pues bien, en el artículo 29 se determina de manera orgánica dicho pronunciamiento, para comenzar en el artículo 30 a regular cuáles son sus funciones.

Algunas de dichas funciones también se habían relacionado brevemente al desarrollar los artículos precedentes; pero en la norma del artículo 30 se enumeran las funciones básicas que la ley le atribuye a la Jefatura de Gabinete de Ministros, como Autoridad de Aplicación:

En el inciso a) le asigna la función de dictar las normas reglamentarias y de aplicación y la reglamentación establecida en el Decreto 2628/02, en el artículo 6, concreta que se refiere a los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales, y que el art. 14 había previsto entre los recaudos de validez del certificado digital. A ese respecto son varios los estándares reconocidos; pero en uso de la atribución conferida por las normas citadas, la Jefatura de Gabinete de

Ministros ha determinado el empleo del estándar “X.509” en su versión 3[52]. Este formato, como vimos, al comentar el artículo 14, tiene la función informática de enlazar o vincular la clave pública con los datos que permiten identificar al titular de la misma. Remitimos a este respecto a lo desarrollado en nuestro comentario al artículo 14.

En los incisos siguientes se establece la facultad de determinar el procedimiento de firma y verificación, conforme al estándar tecnológico; las condiciones mínimas de emisión de los certificados.

En cuanto a los efectos de la revocación de los certificados, establecido en el inciso c), no se refiere aquí a lo que hemos analizado en los arts. 15 y 19 de la ley, ya que en esa oportunidad se aludía al certificado obtenido por el usuario final del sistema, concretamente, al firmante. Aquí, en cambio, se refiere al efecto de la revocación del certificado del mismo Certificador Licenciado y del Ente Licenciante que, como sabemos, también operan por medio de dicho instrumento digital en el ejercicio de su función certificante y licenciante.

El inciso d, del artículo 30 de la ley 25506 propone la posibilidad de instrumentar acuerdos internacionales para validar las certificaciones que se expidan por certificadores licenciados del País, así como las que se expidan desde el extranjero para producir sus efectos en Argentina. Ya habíamos analizado, cuando nos referíamos al artículo 16 de la ley 25506. En el que habíamos establecido la vocación sinfrónica de la firma digital, muy propia, por otra parte, de los efectos de la globalización o mundialización que estamos viviendo en estos tiempos. Por ello, mediante la atribución conferida en la norma analizada, se coadyuva a que el sistema trascienda las fronteras del país y logre su cometido también respecto de otras naciones, posibilitando la contratación entre personas de distintos países. Para

[52] FARRÉS, Pablo; Ob.cit., pág. 175. LUZ CLARA, Bibiana; Ob.cit. pág. 74.

completar lo relacionado a este inciso remitimos a nuestro análisis del artículo 16 ya citado.

En los incisos e, g, i, y K, del artículo 30, se otorgan a la Autoridad de Aplicación toda la gama de facultades necesarias para ejercer el contralor de los certificadores licenciados y del Ente Licenciante. Dictaminar sobre las pautas de de auditoría, los niveles de licenciamiento; fiscalizar el cumplimiento de la ley y reglamentaciones y aplicar las sanciones que correspondan, según lo reglamentado a partir del artículo 40 de la ley 25506. En los otros incisos, en cambio se prevén facultades de las más variadas, como la de actualizar los valores para las sanciones punitorias de multas, conforme al artículo 43; otorgar y revocar las licencias, esta última medida también como aplicación de la sanción establecida en el artículo 44, que la ley rotula de "caducidad"[53] y homologar los dispositivos de creación y verificación de firmas digitales. Como fácilmente puede advertirse la norma está redactada con un método poco feliz, ya que incisos que hacen al sistema en su funcionamiento estructural, como la homologación de los dispositivos de creación de firma digital y su verificación, aparecen entremezclados con otros que hacen al control posterior de la actividad del Certificador, conforme al inciso h. Pero remarquemos, como lo hemos hecho en otras oportunidades, que esta es una falencia de aparición constante en la ley que comentamos.

Es menester también mencionar aquí a la Oficina Nacional de Tecnologías de información (ONTI) que es el órgano rector en materia de tecnología informática dependiente directamente de la Subsecretaría de la Función Pública de Gabinete de Ministros. Esta oficina, por decreto 1028/03, sustituye al Ente Administrador de firma digital que había sido creado por el artículo 11 del Decreto Reglamentario 2628/02. Es también la entidad

[53] Ya habíamos criticado las expresiones indistintas "caducidad" y "revocación" como si tuvieran el mismo significado. Ver comentario al artículo 22 de esta obra.

asesora en materia técnica en lo que respecta a firma digital y la autoridad que aplica las sanciones establecidas en el artículo 41.

ARTICULO 31. — Obligaciones. En su calidad de titular de certificado digital, la autoridad de aplicación tiene las mismas obligaciones que los titulares de certificados y que los certificadores licenciados. En especial y en particular debe:

a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;

b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;

c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;

d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;

e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.

ARTICULO 32. — Arancelamiento. La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

Conforme a la remisión que la misma ley 25506 efectúa en la norma del artículo 31, se hacen aplicables aquí los dispositivos de los artículos 21 y 25, de los que ya nos hemos ocupado y puntos a los que remitimos para complementar este análisis. El hecho de hacer especial hincapié en las obligaciones que expresamente se mencionan en la norma del artículo 31, obedece a que en dichos incisos se prevén los aspectos que hacen a la confiabilidad del sistema.

En cuanto a los incisos a y b, hay en ellos una relación muy estrecha con lo regulado en la ley 25326, de 2000, de "Protección de Datos personales", tal como habíamos apuntado al referirnos al artículo 21 de la ley 25506. Son de aplicación de manera especial, en relación con la norma que analizamos, los artículos 5 y 6 del citado cuerpo normativo, tal como puntualiza Luz Clara[54].

CAPITULO VII

Del sistema de auditoría

ARTICULO 33. — Sujetos a auditar. El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación.

[54] LUZ CLARA, Bibiana; Ob.cit. pág. 117 y 118.

La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

ARTICULO 34. — Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorías las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

Ya nos habíamos referido brevemente a las auditorías realizadas por la Autoridad de Aplicación, en nuestro análisis del artículo 27, puesto que en la citada norma se genera la obligación, a la Autoridad de Aplicación de diseñar un sistema de auditorías.

Las obligaciones impuestas en las normas precedentes a cada uno de los sujetos intervinientes en el procedimiento de la firma digital, tanto al certificador licenciado, como al Ente Licenciante, deben ser auditadas; es decir inspeccionadas por funcionarios de la Autoridad de Aplicación o por terceros contratados por ésta a esos efectos. El certificador licenciado tiene la obligación de permitir el ingreso de los funcionarios autorizados y enviados por la Autoridad de Aplicación, del Ente Licenciante o de los Auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso, según lo expresamente

determinado en el artículo 21, inc. “r” de la ley 25506 y el artículo 27 inc. “e” que sanciona con la caducidad de la licencia (debería decir “revocación”) al certificador que “(...) no permita la realización de auditorías o inspecciones dispuestas por el Ente Administrador.

La finalidad de estas inspecciones que pueden ser ordinarias, periódicas de rutina o extraordinarias[55], en caso de advertirse alguna anomalía o probable irregularidad en el servicio, es mantener el sistema en estado de confiabilidad y controlar el efectivo cumplimiento de las imposiciones de la ley. Por ello la norma recava especialmente en los elementos básicos para generar confianza; por lo menos deben evaluarse en estas inspecciones de rutina, la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos. Igualmente controlará el cumplimiento efectivo de las especificaciones del manual de procedimientos, el plan de seguridad y, el de contingencia. Recordemos que estos elementos, debieron ser remitidos al Ente licenciante para que previa evaluación y dictamen sobre su aprobación, éste confiera la licencia, según lo que ya hemos anotado en relación al inciso “t” del artículo 21. Las expresiones técnicas, utilizadas en la norma (manual de procedimientos, plan de seguridad y de contingencia, etc.) resultan suficientemente aclaradas en glosario final del decreto reglamentario 2628/2002 (puntos 6 al 10 del glosario). Remitimos a nuestra nota al artículo 21 para completar lo expresado.

[55] No se menciona esta distinción en la ley ni en su reglamentación; pero surge evidente que las inspecciones o auditorías de rutina u ordinarias deberán tener una periodicidad no menor del año calendario. Así surge tangencialmente del Decreto Reglamentario 2628/2002, artículo 27 inc. a), cuando determina como incumplimiento que puede generar la revocación (o caducidad, usando las expresiones legales) de la licencia, el no haber presentado la declaración jurada “anual”. Ver al respecto Farrés, Pablo; Ob.cit. pág. 325. Las auditorías extraordinarias, en cambio, obedecen al hecho de haberse advertido alguna irregularidad que obliga al Ente Licenciante a investigar de manera especial alguna circunstancia.

El artículo 33 no exige que las auditorías sean realizadas directamente por la Autoridad de Aplicación, sino que, siguiendo una tendencia moderna de reconocimiento oficial a la actividad privada[56], posibilita que ésta se valga de terceros habilitados expresamente a esos efectos. Estos terceros no pueden estar dedicados a la prestación de servicios de firma digital, en razón de la incompatibilidad que el sistema genera para evitar el conflicto de intereses, según lo sentado en el artículo 20 del Decreto Reglamentario 2628/02.

Pues bien, en el artículo 34 se mencionan quiénes pueden ser los sujetos que obren como entidades auditoras. Podrán serlo las universidades; los organismos científicos o tecnológicos, nacionales o provinciales. La norma, pareciera imponer, con carácter restrictivo, que sólo pueden ser habilitadas como Entidades Auditoras los organismos y universidades de la Nación o Provincias, según surge de la letra de la ley, por lo que haciendo esa interpretación literal quedarían excluidos las universidades y organismos no oficiales. Sin embargo, siendo la tendencia actual, como decíamos, la admisión de la actividad privada como organismos de control, no creemos acertado el dispositivo al haber usado esas expresiones ("nacionales o provinciales") ni que haya sido esa la intención del legislador. Una vez acreditadas su solvencia y capacitación no deberían existir reparos en admitir también a los entes privados; sobre todo en lo referente a las Universidades que han debido sortear la calificación expresa del Ministerio respectivos para poder funcionar como tales, garantizando por esta circunstancia la idoneidad de sus servicios[57].

[56] FARRÉS, Pablo; Ob.cit. pág. 325.
[57] Por otra parte, el artículo 8 del Decreto Reglamentario 2628/02, menciona expresamente a las Universidades privadas reconocidas por el Estado, a cuyos egresados concede la posibilidad de integrar la Comisión Asesora regulada a partir del artículo 35 de la ley 25506.

Igualmente se permite que sean Entidades Auditoras, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

Estas normas deben correlacionarse con las de los articulos 18 y 19 del Decreto Reglamentario 2628/02 que establece que a los fines de seleccionar las entidades de auditoria, la Jefatura de Gabinete de Ministros convocará a concurso público. Las entidades interesada en prestar el servicio de auditoría determinado en esta ley, podrán presentarse cumpliendo con las exigencias previstas en un pliego estándar de precalificación que debe elaborar la dicha Jefatura. Todo ello en cumplimiento del artículo 18 del Decreto Reglamentario.

Luego de realizada la auditoría, el Ente Auditor deberá presentar ante la Autoridad de Aplicación el informe respectivo que, en forma de acta, determinará si los sistemas utilizados por el certificador licenciado cumplen o no con los requerimientos de la ley 25506 y sus reglamentaciones. El resultado de la auditoría, en sus aspectos relevantes, debe ser publicitado en la página web del certificador licenciado, conforme lo vimos al comentar el artículo 21[58].

CAPITULO VIII

De la Comisión Asesora para la Infraestructura de Firma Digital

ARTICULO 35.- Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de

[58] LUZ CLARA, Bibiana; Ob.cit. pág. 121.

carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.

Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez.

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas.

Nos habíamos referido brevemente ya a la Comisión Asesora para la infraestructura de la firma digital, cuando nos referimos a la organización institucional que la ley regula en tres normas arts. 26 a 28. El artículo 28 crea la Comisión que en los arts. 35 y 36 se regula en cuanto a su integración y funciones. Esta Comisión funciona en el ámbito de la Jefatura de Gabinete de Ministros (artículo 7, Decreto Reglamentario 2628/02).

En el artículo 35 se establece en primer lugar la integración de la citada Comisión, determinando que debe ser multidisciplinaria; lo que constituye todo un acierto, dado que se requieren aquí, en materia de firma digital, distintas especialidades afines a la actividad, para que el sistema

brinde realmente todos sus frutos. Deben pues estar vinculados al régimen especialistas en informática, en criptografía, en electrónica, en derecho, en contabilidad, etc. Por ello el Decreto reglamentario (artículo 8) establece que *"La Comisión Asesora para la infraestructura de Firma Digital estará integrada multidisciplinariamente por profesionales de carreras afines a la actividad, de reconocida trayectoria y experiencia, provenientes de organismos del Estado Nacional, Universidades, Cámaras, Colegios u otros entes representativos profesionales. (...)".*

El número de integrantes de la Comisión Asesora no podrá ser superior a siete; y se seleccionarán y designarán por el Poder Ejecutivo, entre los profesionales de reconocida trayectoria y experiencia de las Universidades, Cámaras, Colegios u otros entes representativos de profesionales. El decreto reglamentario, en el artículo 8, exige recaudos básicos para integrar la Comisión: a) Título universitario correspondiente a carrera profesional de duración superior a cuatro años; b) Antecedentes académicos y profesionales en la materia[59]. Su desempeño en las funciones dura cinco años, renovables sólo por un período más y su tarea no es remunerable ya que el cargo es "ad honorem", según previsión expresa del Decreto Reglamentario, artículo 9.

Esta Comisión se reunirá como mínimo cada tres meses y de su actuación y debates, se dejará constancia en el Libro de Actas de la Comisión que deberá llevarse por orden cronológico, y del que surgirán también las recomendaciones y disidencias producidas entre sus miembros. El resultado del debate y decisiones deberá elevarse a la Subsecretaría de la Gestión Pública dentro de los diez días de concluido el análisis del tema.

[59] No se especifica en la norma si los recaudos son disyuntivos o conjuntivos (lo que es común en las leyes y reglamentaciones modernas). Si estamos a la letra de la norma deberemos pronunciarnos que son acumulativos o conjuntivos. No bastará pues con el título universitario, sino que además se requerirán los antecedentes mencionados en b).

Las decisiones de la Comisión se adoptarán por simple mayoría de los miembros presentes con un quórum mínimo de cuatro miembros.

Un punto muy elogiable de la ley es que admite de manera orgánica la consulta acerca del funcionamiento del sistema de firma digital, no sólo a los organismos, cámaras empresariales, asociaciones de consumidores, etc. sino fundamentalmente al usuario directo, para lo cual se efectuarán audiencias públicas, se recibirán aportes por escrito o virtuales, y se abrirán foros de debate vía Internet. El artículo 10 del Decreto Reglamentario establece la necesidad de que esta Comisión articule los medios necesarios que permitan mantener un "intercambio fluido" con los consumidores sobre el sistema, a los fines de recibir todos los aportes y opiniones[60]. El resultado de estas consultas y aportes deberá ser formalmente informado a la Autoridad de Aplicación.

ARTICULO 36. — Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

a) Estándares tecnológicos;

b) Sistema de registro de toda la información relativa a la emisión de certificados digitales;

c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;

[60] LUZ CLARA, Bibiana; Ob.cit. pág. 125, menciona el sitio "www.pki.gov.ar", como ejemplo de consulta pública realizada por la Comisión, sobre requisitos mínimos para políticas de certificación, perfil mínimo de certificados y listas de certificados revocados, procedimiento de licenciamiento y licencias.

d) Metodología y requerimiento del resguardo físico de la información;

e) Otros que le sean requeridos por la autoridad de aplicación.

La norma regula sobre las funciones de la Comisión Asesora que, como técnica que es, se referirá a todos los aspectos vinculados a la firma digital. Los estándares tecnológicos aludidos en la norma, son aquellos a los que nos habíamos referido en nuestro análisis del artículo 14. Habíamos dicho allí que la autoridad encargada de determinar qué estándares reconocidos internacionalmente se usarán a los fines de la ley 25506, es la Jefatura de Gabinete de Ministros, según lo expresa el art. 6, inciso a) del Decreto 2628/02: "Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer: a) Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales. (...)"; pues bien creada la Comisión Asesora que estamos analizando, a partir del artículo 28, resulta ser la delegada de tal función.

Los estándares reconocidos son varios; pero se ha consensuado el empleo del estándar "X.509" en su versión 3[61]. Este formato estándar tiene la función informática de enlazar o vincular la clave pública con los datos que permiten identificar al titular de la misma.

Habíamos expresado también la necesidad de registrar y conservar toda la información referida a la emisión de certificados por parte del certificador, artículo 19 inc. d; y por ello la norma analizada exige a la Comisión Asesora que efectúe las recomendaciones apropiadas para llevar

[61] FARRÉS, Pablo; Ob.cit., pág. 175. LUZ CLARA, Bibiana; Ob.cit. pág. 74.

dicho registro, así como la metodología y requerimiento del resguardo físico de la información.

El artículo 21, dedicado a las obligaciones del Certificador Licenciado, impone en el inciso a, la necesidad de que éste brinde la información adecuada al usuario, no sólo de manera directa, sino también a través de la política de certificación, cuyo sentido técnico explicáramos también en nuestro comentario al artículo 19 inciso n. En atención a ello el artículo 36 que analizamos dispone que sea la Comisión Asesora la que dicte las recomendaciones apropiadas respecto al contenido mínimo de la información a los usarios en cuanto a los términos de las citadas políticas.

Esta norma debe correlacionarse con los arts. 14, 19, 21 de la ley.

CAPITULO IX

Responsabilidad

ARTICULO 37. — Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente.

La norma cuyo análisis abordamos, y quizás debamos decir, todo el capítulo IX, genera grandes interrogantes. En primer lugar nos preguntamos si realmente era necesaria su inclusión en la ley 25506[62], puesto que el Código Civil ya prevé y de manera bastante acabada, cuáles son los efectos

[62] FARRÉS, Pablo; Ob.cit. pág. 347, dice: “La normativa incluida a instancias de uno de los proyectos nacionales resulta objetable, confusa e innecesaria”.

de los contratos; tanto en sus consecuencias normales, como en las patologías frente al incumplimiento de alguna de las partes de sus obligaciones o deberes. En segundo lugar, también aparece como sobre abundante la reiteración de la responsabilidad por los daños generados, puesto que también en este tema, la regulación civil es clara y contundente, al punto tal que llega a expresar sarcásticamente Farrés que "Si este capítulo no estaba en la ley, tampoco importaba. El certificador iba a responder por los daños y perjuicios que ocasionare, por los incumplimientos, errores u omisiones legislativas (...)"[63].

Son de aplicación las pautas generales civiles, arts. 1137 y 1198 del C.C. Recordemos que el primero de estos artículos nos define el contrato en los siguientes términos: "Hay contrato cuando varias personas se ponen de acuerdo sobre una declaración de voluntad común, destinada a reglar sus derechos". La voluntad común a que alude la norma, aparece en materia de firma digital frente a la solicitud de certificado y emisión del mismo como consecuencia de aquella.

Sin dudas, cada vez que se solicita la expedición de un certificado digital, en los términos del artículo 13, 14 y 19 de la ley 25506, y se expide por el Certificador Licenciado, se genera un contrato que, aplicando las normas civiles, calificaremos de innominado, bilateral, oneroso y consensual. Es innominado porque la ley no lo designa bajo una denominación especial (artículo 1143 del Código Civil); es bilateral porque ambas partes se obligan recíprocamente la una hacia la otra (1138 C.C.); oneroso porque la ventaja que genera a una de las partes le es concedida en razón de que ésta abona al co-contratante certificador un canon que, en este caso, será el arancel o tasa que deberá afrontar por la prestación del servicio (artículo 1139 del

[63] FARRÉS, Pablo; Ob.cit. pág. 351

C.C.). Resulta igualmente un contrato consensual considerando que queda concluido desde la manifestación del consentimiento (artículo 1140 C.C.).

Por efecto del contrato aludido en el artículo que comentamos, se generan obligaciones por las que el solicitante se compromete a abonar el servicio según las tasas preestablecidas y a colaborar en el cumplimiento de los recaudos necesarios para preservar la seguridad del sistema en esa prestación concreta que está por recibir del Certificador licenciado.

Ese deber de colaboración, que no sería técnicamente una obligación, está establecido en la exigencia técnica de configuración del sistema o en el despliegue de una conducta preventiva para evitar que la confiabilidad del mismo fracase. Así se le adjudica el deber de utilizar un dispositivo de creación de firma digital confiable; mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos e impedir su divulgación; solicitar la revocación de su certificado si advierte que pueda estar comprometida la privacidad de los datos de creación de su firma, e informar al certificador el cambio en alguno de los datos contenidos en el certificado digital. Veremos al analizar las responsabilidades del certificador licenciado que se limitará la misma, frente a terceros, en caso de que haya habido defecto u omisión en la información que el titular del certificado le hubiere proporcionado (artículo 39, inc. c). Todo ello en armonía con las llamadas obligaciones del titular del certificado digital, previstas en el artículo 25 de la ley.

Por su parte el Certificador, en cumplimiento de lo solicitado por el usuario y acorde a lo prescripto por ley, debe emitir un certificado conforme a la política de certificación y demás condiciones que la autoridad de aplicación le haya establecido (artículo 19 ley 25506). Igualmente deberá informar previamente a la emisión, las condiciones precisas de utilización del certificado digital, con todas las especificaciones determinadas en el artículo 21 inc. a).

ARTICULO 38. — Responsabilidad de los certificadores licenciados ante terceros.

El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, 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. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

Como sabemos se distinguen dos tipos de responsabilidades en el campo del derecho privado, según la fuente que la haya originado. La responsabilidad por mora o incumplimiento de las obligaciones contraídas y la responsabilidad extracontractual o “aquiliana”. En el primer caso hay un incumplimiento de una obligación que, si genera daño, opera el nacimiento de la obligación de reparar el daño producido; en cambio para que opere la responsabilidad aquiliana se ha producido un hecho dañoso autónomo sin que hubiera obligación previa alguna. En un caso hay previamente un marco contractual y, ulteriormente, el deudor incumple una obligación derivada de ese contrato. En el otro caso, hay un hecho que consiste en la violación de una situación jurídica subjetiva. En el primer caso se protege el interés del acreedor y en el otro el interés del damnificado. Ambos están ubicados en posiciones distintas y por ello las normas jurídicas aplicables son diferentes: La responsabilidad aquiliana o extracontratual, es la sanción que el ordenamiento jurídico prevé contra hechos jurídicos lesivos de la integridad

de las situaciones jurídicas protegidas *erga omnes* por el ordenamiento. Este supuesto también se llama responsabilidad *"aquiliana*" aludiendo a la "lex Aquilia".

Pues bien, como surge fácilmente de la norma que estamos analizando, se prevén los dos tipos de responsabilidad de los que hablábamos en los párrafos precedentes, una de fuente contractual, entre el usuario y su Certificador; y otra extracontractual o "aquiliana", impuesta por la ley que lo vincula a terceros. La circunstancia es lógica si se tiene en cuenta que la responsabilidad no sólo será entre el certificador y el usuario que han contratado conforme a lo que dejamos establecido en el artículo anterior, sino también entre certificadores que no tienen ningún convenio entre ellos.

Para que exista la responsabilidad civil es necesario que concurran los factores que, con ligeras variantes, la doctrina tiene establecidos en número de cuatro[64]; a saber:

a) EXISTENCIA DE UN DAÑO: El principio de la responsabilidad civil que reza *no hay responsabilidad sin daño*, surge del artículo 1067 del Código Civil, cuando expresa que *"No habrá acto ilícito punible para los efectos de este Código, si no hubiese daño causado, u otro acto exterior que lo pueda causar, y sin que a sus agentes se les pueda imputar dolo, culpa o negligencia".* Pues bien para que se pueda reclamar reparación al Certificador será menester que su acción u omisión haya causado un daño. Como ejemplo de uno típicamente producido en el ámbito de la firma digital, podríamos imaginar la divulgación de un importante secreto industrial de una empresa, mantenido en confidencialidad para darle valor

[64] Para analizar las distintas posturas y elementos de la responsabilidad civil que se han dado en doctrina, recomendamos la obra de TRIGO REPRESAS, Félix A. y LÓPEZ MESA, Marcelo J.; "Tratado de la Responsabilidad Civil", Ed. La Ley, Bs. As. 2004; pág. 387 a 393.

comercial, que por el incumplimiento de ciertas conductas impuestas por ley al Certificador, queda a merced de conocimiento de otros empresarios, perdiendo así toda su valía. Igualmente encajaría como válido ejemplo, la mala encriptación del mensaje que deja al descubierto cartas misivas, violándose el derecho a la intimidad, previsto en el artículo 1071 bis del Código Civil[65].

b) ANTIJURIDICIDAD: Se exige, conforme al artículo 1066 del C.C., que exista una norma que prohiba el accionar dañoso mencionado en el punto precedente que, continuando con el ejemplo brindado en el punto anterior, estaría contemplada en el artículo 21, inciso g).

c) RELACIÓN DE CAUSALIDAD: Deberá existir una relación entre el daño y la causa. Se va a exigir una conexión material o, en nuestro caso informática virtual, entre la persona que causó el daño y la persona a quien la ley declara responsable. Ejemplo, que la omisión del Certificador en el cumplimiento de sus deberes, haya sido la que efectivamente causó la divulgación motivo del daño.

d) UN FACTOR DE ATRIBUCIÓN: Debe existir igualmente la posibilidad de atribuir o imputar la responsabilidad por la existencia de culposo o dolo.

En la enumeración contenida en la norma, respecto de las acciones u omisiones dañosas en que incurriere el Certificador, cuando dice *"(...) es responsable (...) por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma (...)"* es

[65] FARRÉS, Pablo; Ob.cit. pág. 348.

evidente que se han destacado especialmente las que se han considerado más importantes; puesto que deben considerarse cualesquiera de las obligaciones que aparecen, tanto en el artículo 21 de la ley 25506, como las que se encuentran enmascaradas en su artículo 19 que alude a las funciones del Certificador Licenciado. También deben considerarse las que surgen del Decreto Reglamentario 2628/02, artículo 24.

Respecto del párrafo final de la norma, que prevé que en caso de producirse el accionar o la omisión causante del daño, corresponderá al Certificador la prueba de su diligencia, Farrés efectúa una simpática crítica, al expresar que la frase encierra una “criptocontradicción”; pues entiende que el certificador jamás podría demostrar diligencia si ha omitido una obligación impuesta por la ley o ha cometido errores. Sin embargo, por el propio Código Civil, hay supuestos en los que se libera de responsabilidad al deudor, aún cuando no ha cumplido o cuando ha cometido errores, por ejemplo cuando exista un caso fortuito (artículo 514 del Código Civil).

Para afrontar el pago de los daños que pudieran ocasionarse, el Decreto Reglamentario 2628/02, en el artículo 29 inc. e), requiere al certificador la información sobre las garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades; y el artículo 30 del citado Decreto exige al Certificador contar con seguros vigentes, conforme a las responsabilidades asumidas. Sólo se liberarán del seguro obligatorio los certificadores licenciados pertenecientes al sector público.

ARTICULO 39. — Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;

b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

Tal como las responsabilidades que, según vimos, surgen de los hechos o de las leyes que imponen las obligaciones, igual ocurre con sus limitaciones una vez impuestas aquellas. Así, en la norma que analizamos, en su inciso a), se determina que las limitaciones a la responsabilidad de los certificadores podrán surgir del propio contrato; es decir de las condiciones de emisión y utilización del certificado expedido, y de la ley que los rija. A estos efectos deben tenerse presentes las normas del Código Civil que prevén que sólo la culpa es factible de ser excusada por convenio de partes, lo que no es permitido respecto del dolo. En efecto, recordemos que el artículo 507 dice: *"El dolo del deudor no podrá ser dispensado al contraerse la obligación"*.

En cuanto al inciso b), éste resulta prácticamente una reiteración del anterior, pues alude a los daños producidos por la utilización no autorizada, si en las condiciones de emisión y utilización del certificado constan las restricciones. Es la misma norma del inciso a) pero redactada en otra forma.

Respecto del inciso c), es la lógica contrapartida de lo que habíamos advertido al mencionar el deber que tienen los titulares de certificados de colaborar, cumpliendo con los recaudos necesarios para preservar la seguridad del sistema en la prestación que está por recibir del Certificador licenciado, si la colaboración se presta inadecuadamente; es decir no informando o informando circunstancias erradas; obviamente sería del todo injusto hacer cargar al Certificador con la responsabilidad por los daños que eventualmente ello causara, tanto al propio titular del certificado como a terceros. Ese supuesto estaría pues limitado, siempre que el Certificador acredite haber obrado con la diligencia necesaria, cuando por ley tiene la obligación de verificar la certeza de la información.

CAPITULO X

Sanciones

ARTICULO 40. — Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley serán realizadas por el ente licenciante. Es aplicable la Ley de Procedimientos Administrativos 19.549 y sus normas reglamentarias.

ARTICULO 41. — Sanciones. El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:

a) Apercibimiento;

b) Multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000);

c) Caducidad de la licencia.

Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación.

El pago de la sanción que aplique el ente licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos, como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

Las responsabilidades que se determinan en las normas de los artículos 37 a 39, no impiden que, además, el Ente Licenciante pueda, previo sumario que él mismo instruya, aplicar al Certificador Licenciado las sanciones que, según el artículo 41 que también se analiza en este capítulo, podrán variar entre: Apercibimiento, multa y caducidad de la licencia, según la gravedad de la falta. La reparación de los daños, tiene un fundamento y una causa diferente; por ello el mismo artículo 41 determina que la sanción y su cumplimiento no liberan al Certificador Licenciado de responder ante los terceros por los daños irrogados.

En todo el trámite para determinar la sanción y su aplicación, la ley 25506, establece que se aplicarán las normas nacionales de procedimiento administrativo; es decir la ley 19549 de 1972, reformada por la 21686 de 1977, y sus reglamentarias (o, aunque la norma no lo diga, las que en el futuro las sustituyan). Esta ley nacional prevé en su artículo 1, postulados básicos, que tiene ya establecidos la doctrina para todo proceso

administrativo. A los fines ilustrativos recordaremos los citados principios básicos sentados en la ley 19549 que interesan especialmente a los fines de la ley 25506:

1- Impulsión e instrucción de oficio. 2- Celeridad, economía, sencillez y eficacia en los trámites Este régimen comprende la potestad de aplicar multa de hasta cien pesos -cuando no estuviere previsto un monto distinto en norma expresa- mediante resoluciones que, al quedar firmes, tendrán fuerza ejecutiva. 3- Excusación de la inobservancia por los interesados de exigencias formales no esenciales y que puedan ser cumplidas posteriormente. 4- Las actuaciones y diligencias se practicarán en días y horas hábiles administrativos, pero de oficio o a petición de parte podrán habilitarse aquellos que no lo fueren. 5- Los plazos serán obligatorios para los interesados y para la Administración y se contarán por días hábiles administrativos salvo disposición legal en contrario o habilitación resuelta de oficio o a petición de parte. Se computarán a partir del día siguiente al de la notificación. 6- Derecho de los interesados al debido proceso adjetivo, que comprende el derecho a ser oído; exponer las razones de sus pretensiones y defensas antes de la emisión de actos que se refieren a sus derechos subjetivos o intereses legítimos; interponer recursos y hacerse patrocinar y representar profesionalmente; de ofrecer prueba y que ella se produzca, si fuere pertinente, debiendo la administración requerir y producir los informes y dictámenes necesarios para el esclarecimiento de los hechos, todo con el contralor de los interesados y sus profesionales, quienes podrán presentar alegatos y descargos una vez concluido el período probatorio; derecho a una decisión fundada; y derecho a que el acto decisorio haga expresa consideración de los principales argumentos y de las cuestiones propuestas, en tanto fueren conducentes a la solución del caso.

En el artículo 41 se regulan las distintas sanciones que ya hemos mencionado, a las que habría que agregar la de inhabilitación por el término

de diez años para ser titular de licencias de certificador, como complemento ante la sanción de caducidad, según la previsión del artículo 44.

Como también habíamos expresado, la aplicación de la sanción dependerá de la gravedad de la inconducta; siendo el criterio de graduación la reincidencia y la oportunidad en que se hubieren cometido las faltas. La ley delega aquí, en el Decreto Reglamentario 2628/02, el establecimiento de la sanción pertinente, pero en éste nada se determina al respecto. Es la Oficina Nacional de Tecnología de Información (ONTI), como autoridad de aplicación, artículo 30 inc. k), la que cumple la función de Ente Licenciante, conforme al Decreto 1028 de 2003, y por ello es esta oficina la que aplica y gradúa la sanción[66], tal como habíamos adelantado al comentar el artículo 29.

ARTICULO 42. — Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos:

a) Emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;

b) No facilitar los datos requeridos por el ente licenciante en ejercicio de sus funciones;

c) Cualquier otra infracción a la presente ley que no tenga una sanción mayor.

ARTICULO 43. — Multa. Podrá aplicarse sanción de multa en los siguientes casos:

a) Incumplimiento de las obligaciones previstas en el artículo 21;

[66] LUZ CLARA, Bibiana; Ob.cit. pág. 138.

b) Si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causare perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;

c) Omisión de llevar el registro de los certificados expedidos;

d) Omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;

e) Cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la autoridad de aplicación y del ente licenciante;

f) Incumplimiento de las normas dictadas por la autoridad de aplicación;

g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento.

ARTICULO 44. — Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de:

a) No tomar los debidos recaudos de seguridad en los servicios de certificación;

b) Expedición de certificados falsos;

c) Transferencia no autorizada o fraude en la titularidad de la licencia;

d) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;

e) Quiebra del titular.

La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

En estas tres normas que analizaremos en conjunto, se determinan los tipos de sanciones que se prevén en la ley, y a qué faltas o incumplimientos corresponden; desde la menos gravosa, el apercibimiento, hasta la revocación de la licencia y su inhabilitación por diez años.

El artículo 42 comienza con el apercibimiento, la sanción más leve. Frente a la detección de una inconducta por el Certificador Licenciado, la Autoridad de Aplicación apercibe y notifica de la sanción, con lo cual le está advirtiendo que si vuelve a cometer esa misma falta u otra, ya la sanción será más grave. Tal es lo que surge de manera directa del inciso g) del artículo 43, cuando expresa que corresponderá multa frente a la reincidencia de la falta que hubiere motivado apercibimiento.

Los motivos para el apercibimiento son específicamente dos, contemplados en los incisos a y b. En el inciso c se prevé un supuesto por descarte. Es decir si alguna falta no estuviere contemplada en las sanciones más gravosas, corresponderá el apercibimiento del artículo 42 inc. c.

En cuanto al primer supuesto específicamente contemplado, se refiere al hecho de expedir certificados a pesar de no contar con todos los datos que la ley requiere que verifique antes de emitirlo, si tal omisión no lo invalidare legalmente; es decir si no entra en lo contemplado en el artículo 14 que prevé los recaudos de validez de los certificados digitales. No es fácil encontrar un ejemplo de este supuesto, dado que la generalización que efectúa el artículo 43, inciso a), hace que casi todas las inconductas previstas por la ley como falta de cumplimiento a las obligaciones, merezcan

según el citado inciso, la sanción de multa. Pero, de nuestra parte creemos que el inciso a) del 43, constituye sólo una aproximación y no debe interpretarse en sentido literal, por ello el mismo artículo luego menciona faltas que ya estarían contempladas en la generalización del inciso a). Así, nos atrevemos a poner como ejemplo de la falta regulada en el inciso a) del artículo 42, el comportamiento en desacuerdo a lo establecido en el inciso "o" del artículo 21. Recordemos que esta norma obliga al Certificador Licenciado a *"verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales"*. Otro ejemplo lo constituye el incumplimiento a la obligación establecida en la misma norma del artículo 21, inciso que determina que el Certificador Licenciado debe *"Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso."*

En cuanto al otro supuesto contemplado especialmente para hacer aplicable el apercibimiento, se menciona la falta de información al Ente Licenciante que, como se ha establecido en el artículo 30 y 31 de la ley 25506, tiene la supervisión y el control exclusivo de todo el sistema. Se destacan especialmente entre sus funciones y obligaciones, la de fiscalizar el cumplimiento de las normas legales y reglamentarias en relación a la actividad de los certificadores, supervisar la ejecución de los planes técnicos que deben proporcionar los mismos, entre otras. Pues bien, en razón de tales cometidos, el Ente Licenciante está facultado para requerir datos, y la omisión por parte del Certificador de proporcionarlos le hará incurrir en el apercibimiento previsto en la norma que comentamos. Como ejemplo del supuesto reglado, podríamos poner el incumplimiento de lo normado en la

segunda parte del inciso r del artículo 21, inciso r, que determina que el Certificador Licenciado debe *"…Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso."*

La multa, está contemplada en el artículo 43. En el inciso a) de esta norma, como dijimos en párrafos más arriba, se establece con demasiada amplitud que todo incumplimiento a lo establecido en el artículo 21 haría aplicable esta sanción. No creemos que sea así; en primer lugar porque se contemplan en la norma del artículo 21, obligaciones cuyo incumplimiento no amerita la sanción establecida en el artículo 43, tales como la de no facilitar los datos requeridos por el Ente Licenciante en el ejercicio de sus funciones, supuesto previsto en la segunda parte del inc. r) del artículo 21; ya que, según vimos, el artículo 42 inc. b) hace aplicable a esta inconducta sólo apercibimiento; y en segundo lugar, porque de ser así estarían de más los incisos c), e) y f) del artículo 43, puesto que estos supuestos ya estarían contemplados en el inciso "a" al remitirse a cualquier incumplimiento a las obligaciones determinadas en el artículo 21. En efecto, la omisión de llevar un registro de los certificados expedidos, está contemplada en el inciso i y m de la citada norma; y en el inciso r) primera parte del mismo artículo 21, se encuentra contemplada la obligación de permitir el ingreso a la autoridad de aplicación para las auditorías, según vimos en el párrafo precedente. Otro tanto ocurre con la falta contemplada en el inciso f) del artículo que analizamos, pues la norma del artículo 21 inciso w), también incluiría el supuesto de "incumplimiento de las normas dictadas por la autoridad de aplicación" al que alude el inciso f) del artículo 43, en razón de lo cual habría estado ya dentro del inciso a) de esta norma.

De todo ello extraemos como regla interpretativa que el primer inciso debió decir que se aplicará multa, en general, a todo incumplimiento a las

obligaciones atribuidas al certificador en el artículo 21. Estimamos que la expresión “en general”, dará a la norma el sentido correcto, quitándole el rigorismo matemático que, como se vio no corresponde aplicar.

Hay cierta contradicción entre las normas del artículo 43, inciso e) que se refiere a *“cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la autoridad de aplicación y del ente licenciante”* y el artículo 27 del Decreto Reglamentario 2628/02, que determina que corresponde la sanción de caducidad de la licencia *“cuando el certificador licenciado no permita la realización de auditorías o inspecciones dispuestas por el Ente Administrador”*. En efecto, “impedir” y “no permitir” evocan el mismo sentido, no es un mero obstáculo, sino la imposibilidad absoluta de realizar la auditoría por parte del Ente Administrador. Creemos que la interpretación correcta de esta contradicción consiste en considerar que mientras se trate un obstáculo sorteable corresponderá la multa; mientras que si el impedimento es absoluto, deberá aplicarse directamente la caducidad de la licencia.

Respecto a la cuantía de las multas es atribución del Ente Administrador, según lo sentado en el artículo 13 inc. n) del Decreto Reglamentario 2628/02. Los fondos correspondientes a estas multas integran los recursos del Ente Administrador, según lo sentado en el artículo 16 inc. f).

En cuanto a la sanción de caducidad dispuesta en el artículo 44 de la ley 25506, constituye sin dudas la sanción más gravosa y procede en primer lugar, inc. d), cuando hay reincidencia de alguno de los supuestos previstos en el artículo 43 (multas); y en los demás casos previstos en sus restantes incisos. Como puede advertirse de su lectura con la gravedad de la sanción impuesta a cada una de las faltas enumeradas en la norma, se procura el

afianzamiento de la llamada “confianza digital” que es uno de los principios prioritarios del legislador, para que realmente el sistema sea utilizado. Por ello se mencionan los casos extremos, algunos demasiado genéricos, como el del inciso a), que alude a la falta de recaudos que hacen a la seguridad en el servicio de certificación; otros más específicos como el supuesto previsto en el inciso b): falsedad de los certificados, o lo referido a la transferencia no autorizada o fraude en la titularidad de la licencia previsto en el inciso c). Todas estas patologías repercuten de manera directa en la inseguridad para el usuario, con la gravedad adicional de generar la desconfianza que, como dijimos, intenta prevenir el sistema.

En cuanto al inciso e) de la norma analizada, que prevé la quiebra del titular de la licencia de certificador, obviamente se trata de una consecuencia de la situación del fallido que, a consecuencia de ello, queda desapoderado de sus bienes y, con ello, pierde la posibilidad de garantizar y afianzar su responsabilidad, situación que reñiría con la necesidad de responder por daños causado, según vimos al analizar el artículo 38 de la ley 25506. En efecto, habíamos analizado que para afrontar el pago de los daños que pudieran ocasionarse, el Decreto Reglamentario 2628/02, en el artículo 29 inc. e), requiere al certificador que no pertenece al sector público, la información sobre las garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades; y el artículo 30 del citado Decreto exige al Certificador contar con seguros vigentes, conforme a las responsabilidades asumidas. Pues bien, nada de esto puede cumplirse al estar en estado de quiebra el certificador.

Ya habíamos también adelantado, al analizar el artículo 41, que el complemento a la sanción de caducidad, lo constituye la inhabilitación al Certificador por diez años para ser titular de nuevas licencias.

Deben agregarse a estos supuestos que hacen procedente la sanción de caducidad, los agregados en el Decreto Reglamentario 2628/02, artículo

27: falta de presentación de la declaración jurada anual; falsedad de los datos contenidos en la citada declaración jurada; dictamen desfavorable de auditoría basado en causales graves; informe desfavorable de inspección, por causales graves; y cuando el Certificador impida totalmente (según vimos al analizar los supuestos de multas –artículo 43, inc. e -) la realización de auditorías o inspecciones.

ARTICULO 45. — Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los Tribunales Federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.

La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

ARTICULO 46. — Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso-administrativo Federal.

En las normas de los arts. 45 y 46, cuyo análisis abordamos, advertimos que, con buen criterio práctico, el legislador evita las largas dilaciones que suelen presentarse en los estrados judiciales por cuestiones de competencia en materia recursiva. Directamente aborda el tema y declara la competencia federal para resolver los recursos que el Certificador Licenciado quisiere interponer frente a las sanciones aplicadas que considere injustas.

En cuanto al efecto devolutivo previsto en la norma, la gravedad del mismo para el Certificador Licenciado, dado que implica la efectivización de la sanción mientras pende el pronunciamiento del recurso, obedece a la necesidad de extremar los recaudos tendientes a generar la llamada “confianza digital” que, como dijimos al analizar el artículo 44, constituye uno de los postulados básicos del legislador.

Cualquier litigio motivado en la utilización del sistema de firma digital, entre particulares y el Certificador, será competencia de la Justicia Federal Civil y Comercial. Pero si estuviere involucrado en el problema un organismo público, el asunto será de competencia de la Justicia en lo Contencioso Administrativo Federal, según establece el artículo 46 in fine.

CAPITULO XI

Disposiciones Complementarias

ARTICULO 47. — Utilización por el Estado Nacional. El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

ARTICULO 48. — Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156.

En el artículo 47 se genera la obligación por parte del Estado Nacional de utilizar la tecnología de la firma digital, tanto respecto de sus comunicaciones internas, como respecto de los administrados. Todo ello, conforme a la reglamentación prevista a partir del artículo 37 del Decreto Reglamentario, deberá hacerse en armonía con las pautas que fijen cada uno de los poderes del Estado. Se incluye también a los Estado Provinciales, dado que, conforme al artículo 50 de la ley 25506, se invita a las Provincias a dictar los instrumentos legales pertinentes para adherir al sistema.

En el artículo 48, con una visión de futuro y para lograr la generalización del uso de la firma digital, exige al Estado promover el uso masivo del sistema, en toda la esfera de su jurisdicción y respecto de las entidades comprendidas en el artículo 8 de la ley 24156. En este punto corresponde remarcar que ya desde el año 1998 el Estado estaba encaminado a la "despapelización" de los trámites y optimización de sus actividades por vía informática y soporte digital[67]. Da prueba de ello el Decreto 427/98 que fue el instrumento que creo la infraestructura de firma digital para el Sector Público Nacional. Este decreto, hoy derogado por el

[67] LUZ CLARA, Bibiana; Ob.cit. pág. 147.

Decreto Reglamentario 2628/02 al que hemos venido refiriendo, puede considerarse pionero en el tema en toda América Latina[68].

En cuanto a la ley 24.156/1992, a la que alude el artículo 48, es la ley de administración financiera, que rige la forma de administrar todos los organismos públicos y también las empresas en las que el Estado tenga participación mayoritaria en el capital o en la toma de decisiones.

El artículo 8 de la ley 24156, modificado por ley 25827 de 2003, considera integrado el Sector Público Nacional por: a) Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social; b) Empresas y Sociedades del Estado que abarca a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias. c) Entes Públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones. d) Fondos Fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional.

Según el artículo 48 que comentamos, en 2006 debería haber estado implementado el sistema de firma digital en todos los poderes del Estado; posibilitando que tanto las leyes, decretos, sentencias y resoluciones administrativas usaran la firma digital para generar instrumentos auténticos y

[68] FARRÉS, Pablo; Ob.cit. pág. 372.

con pleno efecto ejecutivo, contribuyendo así a la llamada “despapelización” del estado. Otro tanto se prevé para los organismos enumerados en el artículo 8 de la ley 24156, modificado por el artículo 8 de la ley 25827, cuya transcripción hicimos en el párrafo precedente.

ARTICULO 49. — Reglamentación. El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

ARTICULO 50. — Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

Más de un año después de la publicación de la ley 25506, recién el Poder Ejecutivo dictó el Decreto 2628 de 2002 al que hemos venido aludiendo y relacionando con cada una de las normas de la ley. El motivo de la demora, como bien pone de resalto Farrés[69], obedeció a la situación conflictiva del País con motivo de la renuncia del Presidente de la Nación, en el entorno caótico que se dio en el citado año. Este Decreto 2628/02 ha sido objeto de correlación y análisis en cada uno de los artículos de la ley que resultaba necesario concordarlo, en razón de lo cual carece de interés aquí referirnos a su contenido.

En cuanto al artículo 50 de la ley, efectúa una invitación a las Provincias a dictar los instrumentos necesarios para adherir al sistema. Sin embargo, cabe acotar que el Decreto Reglamentario 2628/02, considera obligatorio el precepto, cuando en el artículo 37, se refiere a las Administraciones Públicas Provinciales. Bien es cierto que esta alusión puede interpretarse también como abarcando sólo la relación entre Nación y

[69] FARRÉS, Pablo; Ob.cit. pág. 380.

Provincias; pero ello no le quita cierto avasallamiento de la ley nacional sobre las autonomías provinciales.

ARTICULO 51. — Equiparación a los efectos del derecho penal. Incorpórase el siguiente texto como artículo 78 (bis) del Código Penal:

Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.

ARTICULO 52. — Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo para que por la vía del artículo 99, inciso 2, de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

ARTICULO 53. — Comuníquese al Poder Ejecutivo.

ANEXO

Información: conocimiento adquirido acerca de algo o alguien.

Procedimiento de verificación: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

a) que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante;

b) que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante;

c) la verificación de la autenticidad y la validez de los certificados involucrados.

Datos de creación de firma digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

Datos de verificación de firma digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

Dispositivo de creación de firma digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

Políticas de certificación: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

Técnicamente confiable: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos:

1. Resguardar contra la posibilidad de intrusión y/o uso no autorizado;

2. Asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;

3. Ser apto para el desempeño de sus funciones específicas;

4. Cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;

5. Cumplir con los estándares técnicos y de auditoría que establezca la Autoridad de Aplicación.

Clave criptográfica privada: En un criptosistema asimétrico es aquella que se utiliza para firmar digitalmente.

Clave criptográfica pública: En un criptosistema asimétrico es aquella que se utiliza para verificar una firma digital.

Integridad: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital.

En el ámbito del derecho penal, dominado por el principio de tipicidad, si la norma no menciona y describe de manera específica y precisa el ilícito punible, no podrá aplicarse sanción penal alguna. Una sanción no puede aplicarse por analogía para casos similares. El principio “nulla pena nullo crimen sine previa lege” obliga al legislador de un nuevo instituto jurídico a determinar concretamente la redacción penal del tipo, acorde con ese nuevo instituto. Al respecto cabe advertir que la firma digital, por ley, reemplaza o

puede reemplazar la firma holográfica, en razón de lo cual correspondería actualizar todas las normas penales que se refieren a la falsificación de documentos y firmas.

Sin embargo el legislador de la 25506 adoptó un criterio práctico al incorporar al Código Penal el artículo 78 bis, por el cual cada vez que aparezcan en una norma penal la expresiones “firma”, “suscripción”, “documento”, “instrumento privado” o “certificado”, dicha norma estará inmersa en el tipo reglamentado en el artículo en el que aparezca. Así resultan involucrados en estos delitos de tipo informático, los artículos 289, inc.1 sobre falsificación de firmas; los artículos 292, 293, 293 bis; 295 y 296, referidos a la falsificación de documentos en general y el artículo 174 inciso 2º que regula la llamada circunvención de incapaces, entre otros.

En cuanto al artículo 52, la autorización en él contenida al Poder Ejecutivo para actualizar los contenidos del anexo (“glosario”), para evitar que éstos no respondan ya a las nuevas tecnologías, responde a una necesidad imperiosa. En efecto, pocas disciplinas y técnicas avanzan tan rápidamente como las referidas o relacionadas con la informática; se trata de un avance en aceleración progresiva; en razón de lo cual mientras más se perfecciona, más rápido pasa a la obsolescencia. Obviamente si queremos que el glosario aporte a la técnica legislativa y a la interpretación normativa, deberá usar toda la terminología nueva que, acorde con el avance tecnológico e informático, se vaya generando.

Recordemos que el artículo 99 de la Carta Magna es el que acuerda las atribuciones al Poder Ejecutivo; y el inciso 2, al que alude la norma del artículo 52 que estamos analizando, es que expresa que *“El Presidente de la Nación tiene las siguientes atribuciones: (...) 2. Expide las instrucciones y reglamentos que sean necesarios para la ejecución de las leyes de la Nación, cuidando de no alterar su espíritu con excepciones reglamentarias”.*