AUTORIDADES CERTIFICADORAS EN LA CONTRATACIÓN ELECTRÓNICA

JOSÉ ANTONIO MÁRQUEZ GONZÁLEZ *

ABREVIATURAS

ABA	<i>American Bar Association (USA)</i>
ANNM	<i>Asociación Nacional del Notariado Mexicano, A. C.</i>
ANSI	<i>American National Standards Institute</i>
CCA	<i>Controller of Certification Authorities</i>
CCDF	<i>Código Civil del Distrito Federal (México)</i>
CCF	<i>Código Civil Federal (México)</i>
CCo	<i>Código de Comercio (México)</i>
CFPC	<i>Código Federal de Procedimientos civiles (México)</i>
CISG	<i>Convention on International Sale of Goods (UNCITRAL)</i>
CNUDMI	<i>Comisión de las Naciones Unidas para el Derecho Mercantil Internacional</i>
EC	<i>Entidades de Certificación</i>
EDI	<i>Electronic Data Interchange</i>
ETA	<i>Electronic Transaction Act (Singapur)</i>
ETR	<i>Electronic Transaction Regulations (Singapur)</i>
IAN	<i>International Attorney-Notaries</i>
INFOSEL	<i>Informática Selectiva, S. A. de C. V.</i>
INP	<i>International Notarial Practitioner</i>
ISO	<i>International Standards Organization</i>
ITU	<i>International Telecommunications Union</i>
IuKDG	<i>Informations-und Kommunikationsdienste-Gesetz</i>
LFPC	<i>Ley Federal de Protección al Consumidor (México)</i>
LMCE	<i>Ley Modelo sobre Comercio Electrónico (UNCITRAL)</i>
NCCUSL	<i>National Conference of Commissioners on Uniform State Laws</i>
NIST	<i>National Institute of Standards and Technology (USA)</i>
PCCI	<i>Principios sobre los Contratos Comerciales Internacionales (UNIDROIT)</i>
SECOFI	<i>Secretaría de Comercio y Fomento Industrial</i>
SiG	<i>Signaturgesetz (Alemania)</i>
TDG	<i>Teledienstegesetz (Alemania)</i>
TDDSG	<i>Teledienstedatenschutzgesetz (Alemania)</i>
UNCITRAL	<i>United Nations Commission on International Trade Law</i>

* Notario de Orizaba y profesor en la Universidad Veracruzana.

INTRODUCCIÓN

Me propongo examinar aquí los aspectos más característicos de una figura muy especial dentro del marco general de la contratación electrónica. Me refiero a las entidades certificadoras. Entiendo por ellas a las personas individuales o jurídicas formalmente habilitadas para constatar ciertos hechos de naturaleza informático-jurídica con relación a los sujetos intervinientes en la contratación electrónica.

Utilizaré el método comparativo y, por tanto, haré un repaso de las leyes más importantes que se han dictado en los últimos años, aunque sólo deteniendo mi atención precisamente en este punto. Decidí elegir solamente las más representativas o aquellas que han tenido una notable influencia. En consecuencia, estudiaré incluso las leyes modelo o guías que se han expedido, por su pretensión de uniformidad legislativa.

Como al final se verá, el examen ha resultado disímbolo. Pero esto mismo es enriquecedor y valioso para el investigador. Cada país y cada sistema económico se ven necesariamente reflejados en la forma de regular las transacciones electrónicas en un mundo, sin embargo, cada vez más pequeño e interrelacionado. Deben sumarse a esto la extrema complejidad del problema a tratar y los cambios intempestivos que resultan de los propios avances tecnológicos y el consecuente impacto en su regulación legal.

Sea como fuere, el trabajo mantiene el propósito final de encontrar los elementos esenciales de una figura que se presenta a la vez como de indispensable presencia y de versátil expresión. Significa también la recuperación del elemento humano fundamental en todo tipo de transacciones, especialmente frente a la tecnología avasallante que es característica de nuestra época.

No me parece que pueda ponerse seriamente en duda la necesidad de la existencia de una figura centralizadora y confiable que aporte los elementos básicos de confianza, seguridad y certeza en la contratación electrónica fría e impersonal.

La historia nos enseña, por otra parte, que este elemento de certeza no puede quedar, en modo alguno, desvinculado del negocio. En efecto, ha existido siempre la necesidad de un elemento externo al negocio, pero inseparable de él, que autentique la intención negocial de las partes y su recepción documental en un medio físico que lo hace perdurar en el tiempo y lo mantiene como recurso adicional para el caso eventual de controversia.

El elemento humano ha jugado, así, un papel entrañable e inescindible con el elemento técnico. Desde este último punto de vista, se pueden plantear dos cuestiones: ¿dónde se escribe? ¿con qué se escribe? Tales muestras forman un binomio *ad hoc*, es decir, hechos el uno para el otro.

A ello debe añadirse la utilización de una marca, signo o sello que plasma la autenticidad del medio físico utilizado. Por último, el círculo se completa con la consideración final del elemento humano, es decir, del escriba o amanuense que anota el acto, le impone su marca peculiar y, sólo al final de una larga evolución, responde de su fidelidad y certeza.

¿Dónde se escribe? Desde la antigüedad más remota se encuentran inscripciones en piedra y en hueso, muy aprovechables en este punto por su condición imperecedera. De hecho, es gracias a esta circunstancia que hemos podido conocer acerca de ellas. Sin embargo, también se ha escrito en tablillas frágiles de barro cocido y luego en bronce, en mármol y en tablillas de madera recubiertas de cero o loza finamente pulidas. Después se ha escrito en hojas de papiro enrollado y en pergaminos o cueros de animales.

La invención del papel (confeccionado a base de arroz, madera, algodón, etc.) no tuvo lugar sino hasta bien entrada la época medieval. Los indígenas de la América precolombina dibujaban en la corteza del amate. Se haría popular luego el uso del papel grueso y rugoso conocido como “papel de estraza” y que luego se convertiría en los pliegos tersos, lustrosos e impecablemente cortados de nuestras hojas *bond*. Casi inmediatamente irrumpió la novedad del papel reciclado para, de pronto, desembocar en la realidad mágica de la memoria electrónica y del espacio cibernético.

¿Con qué se escribe? Nuestros antepasados usaron el cincel, el buril, los punzones y los estiletos romanos de metal o de junco; cada uno de ellos particularmente apropiado al elemento físico que plasmaba la escritura. Fueron populares los pinceles con cerdas animales, luego reemplazados por la pluma de ganso que adorna con frecuencia las pinturas medievales.

Después, los albores del Renacimiento contemplaron la invención de un artefacto capaz de acomodar caracteres (primero de madera y luego de metal) que se utilizaban para componer palabras. Los lápices con barra de carbón fueron inseparables en nuestra niñez, pero también lo fueron las plumas y los modernos bolígrafos, mientras las máquinas de escribir irrumpían en las oficinas modernas. Después de una efímera popularidad, las máquinas de escribir pasaron a ser reemplazadas por modernísimas procesadoras de texto y computadoras personales que reducen el acto de escribir, grabar o pintar, a pulsaciones que almacenan información en combinaciones de *bits*.

¿Y qué decir acerca del signo o sello? Sabemos que en Mesopotamia los contratantes ponían una marca personal en sus tablillas y, en su defecto, hasta una pequeña marca con la uña. Frecuentemente, el propio escribano incluía su signo personal. En la Edad Media era común utilizar entre los nobles y caballeros los anillos sellados o imponer signos secretos o cruces religiosas en los escritos. Se juraba también con gestos y actitudes místicas tocando los Evangelios, acariciando la cruz o aferrando la espada. Y aun en los actuales testamentos cerrados pueden seguirse huellas de la costumbre de imponer marcas o signos secretos y misteriosos. En el derecho norteamericano se utilizan todavía algunos pocos contratos “como si fueran sellados” y nuestro actual sello notarial es un símbolo indiscutible del poder del Estado.

De todo esto se desprende que el material donde se escribe, el instrumento para hacerlo, la utilización de un signo o marca y, por último, la presencia de un funcionario (redactor, consejero o autenticador legal), forman la estructura que a lo largo de la historia ha servido de base en la celebración de los actos y negocios jurídicos.

No puede ser distinto en la era de la contratación electrónica: podrá escribirse en la mágica realidad del cyber-espacio; podrán utilizarse —almacenados en minúsculos *chips*— pulsaciones electrónicas para hacerlo; podrá también alterarse el *signus* medieval hasta convertirlo en un código indescifrable de combinaciones alfanuméricas. Todo ello ha podido hacerse, sin duda, y previsiblemente se seguirá haciendo en el emocionante futuro que nos aguarda.

Pero hay algo que no ha cambiado al final de todo, la presencia de un elemento humano confiable y seguro seguirá siendo —así lo creo— absolutamente indispensable. La razón es clara: ni el material usado, ni la técnica para escribir sobre él, ni la utilización

de signos o marcas misteriosos, pueden por sí mismos conferir el carácter de auténtico a un mero documento físico. Tal agregado sobreviene, en efecto, de un elemento que no tiene representación física alguna y que sólo puede residir en la honestidad de su intervención. Una intervención regulada, por otra parte, por estrictos controles de seguridad que corren al parejo de la responsabilidad depositada en ellos.

Así, la presencia de estas autoridades de certificación y particularmente del notario representa, al final, la combinación armoniosa de las nuevas tecnologías del proceso telemático con el elemento de confiabilidad, seguridad y certeza de alguien que, *ab origine*, goza de estos atributos.

1. REAL DECRETO-LEY 14/1999, DE 17 DE SEPTIEMBRE, SOBRE FIRMA ELECTRÓNICA, ESPAÑA, 1999

Como se sabe, la Unión Europea adoptó el 22 de abril de 1999, en la sesión del Consejo de Ministros de Telecomunicaciones, una posición común respecto del proyecto de Directiva del Parlamento Europeo y del Consejo para Firmas Electrónicas.

En este marco, el gobierno español expidió a su vez un decreto que, en veintiocho artículos, regula la prestación de los servicios de certificación y el control de su actividad.

En términos de lo dispuesto en el art. 1º, “Este Real Decreto-ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España”.

Para mis propósitos es importante aclarar que en su capítulo de definiciones se establece que “Prestador de servicios de certificación es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica”. Estrechamente relacionados con esta definición están los conceptos de “certificado” y “acreditación voluntaria del prestador de servicios de certificación”:

Certificado: Es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

Certificado reconocido: Es el certificado que contiene la información descrita en el artículo 8º y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12.

Acreditación voluntaria del prestador de servicios de certificación: Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

Uno de los puntos que más llama la atención en este real decreto es el que posibilita al sector empresarial la prestación de los

servicios de certificación en régimen estricto de libre competencia. Además, debe recordarse que estos servicios no se encuentran sujetos a autorización previa y no se establece ningún tipo de restricción para otros servicios de certificación siempre y cuando procedan de algunos de los estados miembros de la propia Unión Europea.

Así, el gobierno avala el establecimiento de “sistemas voluntarios de acreditación” de los prestadores de servicios mediante un registro dependiente del Ministerio de Justicia.

Al efecto, debe formularse una solicitud de inscripción a la cual se anexará la documentación necesaria en términos del reglamento. Este registro es público y puede ser consultado por vía telemática, previo el pago de una tasa.¹

El certificado respectivo, cuyo nombre técnico es el de “certificado reconocido”, debe reunir los siguientes requisitos:

ART. 8º.—Requisitos para la existencia de un certificado reconocido.

1. Los certificados reconocidos, definidos en el artículo 2.j) de este Real Decreto-ley, tendrán el siguiente contenido:

- a) La indicación de que se expiden como tales.
- b) El código identificativo único del certificado.
- c) La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral.
- d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.
- f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.
- g) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario.
- h) El comienzo y el fin del periodo de validez del certificado.
- i) Los límites de uso del certificado, si se prevén.

¹ En 1999, esta tasa aplicable al reconocimiento de acreditaciones y certificaciones ascendía a la cantidad de \$47,500 pesetas por cada certificación reconocida. Esta cantidad resultaba equivalente a \$285,48 euros. No tengo conocimiento de que haya sido actualizada hasta la fecha. Desde luego, es sujeto pasivo de la imposición la persona natural o jurídica beneficiada con el reconocimiento o acreditación oficial.

j) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

2. La consignación en el certificado de cualquier otra información relativa al signatario, requerirá su consentimiento expreso.

Estos certificados tienen una validez máxima de cuatro años, contados a partir de la fecha de expedición. Además, la ley establece en forma taxativa cuáles son las causas en virtud de las cuales quedan sin efecto, así como la suspensión de los mismos. Por otra parte, tienen equivalencia legal en cualquier otro país que no sea miembro de la Unión Europea, siempre que reúnan algunas condiciones específicas.

¿Cuáles son las obligaciones de los prestadores de servicios de certificación? Los arts. 11 y 12 las enumeran exhaustivamente en los términos siguientes:

ART. 11.—Obligaciones de los prestadores de servicios de certificación. Todos los prestadores de servicios de certificación deben cumplir las siguientes obligaciones:

a) Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre o por cuenta suya, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho. Se exceptúan de esta obligación los prestadores de servicios de certificación que, expidiendo certificados que no tengan la consideración de reconocidos, se limiten a constatar determinadas circunstancias específicas de los solicitantes de aquéllos.

b) Poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica.

c) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite.

d) Informar, antes de la emisión de un certificado a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial.

e) Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o pérdida de vigencia de sus efectos. A dicho registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que los soliciten, cuando así lo autorice el signatario.

f) En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo con la antelación indicada en el

apartado 1 del artículo 13, a los titulares de los certificados por ellos emitido y, si estuvieran inscritos en él, al Registro de Prestadores de Servicios del Ministerio de Justicia.

g) Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.

h) Cumplir las demás normas previstas, respecto de ellos, en este Real Decreto-ley y en sus normas de desarrollo.

ART. 12.—Obligaciones exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos.

Además de cumplir las obligaciones establecidas en los artículos 7 y 11, los prestadores de servicios de certificación que expidan certificados reconocidos, han de cumplir las siguientes:

a) Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.

b) Demostrar la fiabilidad necesaria de sus servicios.

c) Garantizar la rapidez y la seguridad en la prestación de servicio. En concreto, deberán permitir la utilización de un servicio rápido y seguro de consulta de Registro de certificados emitidos y habrán de asegurar la extinción o suspensión de la eficacia de éstos de forma segura e inmediata.

d) Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

e) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

f) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación.

g) Disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en este Real Decreto-ley y, en particular, para afrontar el riesgo de la responsabilidad por daños y perjuicios. Para ello, habrán de garantizar su responsabilidad frente a los usuarios de sus servicios y terceros afectados por éstos. La garantía a constituir podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un seguro de caución.

Inicialmente, la garantía cubrirá, al menos, el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada prestador de servicios de certificación. Teniendo en cuenta la evolución del mercado, el Gobierno, por Real Decreto, podrá reducir el citado porcentaje, hasta el 2 por 100.

En caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de certificados que emita el prestador de servicios de certificación, la garantía a constituir cubrirá, al menos, su responsabilidad por un importe de 1.000.000.000 de pesetas (6.010.121,04 euros). El gobierno, por Real Decreto, podrá modificar el referido importe.

h) Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años. Esta actividad de registro podrá realizarse por medios electrónicos.

i) Antes de expedir un certificado, informar al solicitante sobre el precio y las condiciones precisas de utilización del certificado. Dicha información, deberá incluir posibles límites de uso, la acreditación del prestador de servicios y los procedimientos de reclamación y de resolución de litigios previstos en las leyes y deberá ser fácilmente comprensible. Estará también a disposición de terceros interesados y se incorporará a un documento que se entregará a quien lo solicite. Para comunicar esta información, podrán utilizarse medios electrónicos si el signatario o los terceros interesados lo admiten.

j) Utilizar sistemas fiables para almacenar certificados, de modo tal que:

1. Sólo personas autorizadas puedan consultarlos, si éstos únicamente están disponibles para verificación de firmas electrónicas.

2. Únicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones.

3. Pueda comprobarse la autenticidad de la información.

4. El signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambios técnicos que afecten a los requisitos de seguridad mencionados.

k) Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando este Real Decreto-ley y sus disposiciones de desarrollo, en el ejercicio de su actividad.

La responsabilidad de estos prestadores de servicios, desde luego, se extiende a los daños y perjuicios causados a cualquier persona en el ejercicio de su actividad, conforme a las normas generales sobre culpa contractual o extracontractual, además de lo establecido en las leyes sobre protección al consumidor.

Un dato importante tiene que ver con la vigilancia de los propios prestadores de servicios de certificación. Ya he dicho que el Registro de Prestadores de Servicio de Certificación depende del Ministerio de Justicia. Sin embargo, la supervisión de los mismos compete, en cambio, al Ministerio de Fomento, a través de la Secretaría General de Comunicaciones. La Secretaría puede actuar en

forma oficiosa o mediante petición expresa del Ministerio de Justicia, cualquier otro órgano oficial o incluso particular interesado. Correlativamente a esta obligación de supervisión, los prestadores de servicio de certificación tienen la obligación de facilitar no solamente la información necesaria, sino también los medios precisos para el adecuado cumplimiento de la función gubernamental.

El título restante se refiere a las infracciones y sanciones. Éstas se dividen, por cierto, en muy graves, graves y leves y están directamente relacionadas con el beneficio bruto obtenido y con multas, en el caso de infracciones leves, por el importe de hasta dos millones de pesetas, además de la publicación de la resolución en el Boletín Oficial del Estado y en los periódicos de difusión nacional. La autoridad competente para el conocimiento y eventual imposición de las sanciones es la propia Secretaría General de Comunicaciones del Ministerio de Fomento.

Es importante precisar, que los prestadores de servicios de certificación ya establecidos tendrán necesariamente que adaptarse al nuevo marco legal. Se fija el límite de un año, pero se previene expresamente que los certificados expedidos que ya hayan surtido efectos conservarán su validez.

Por último, según el Boletín Oficial del Estado Nº 45 de fecha 22 de febrero de 2000, se dictó el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica, el cual completa y precisa una gran parte de las disposiciones anteriores.

2. *ELECTRONIC TRANSACTION ACT*, SINGAPUR, 1998

La Ley de Transacciones Electrónicas de Singapur fue expedida en 1998 (*Electronic Transactions Act*). Contiene un total de doce partes que se refieren a notas preliminares, registros electrónicos y firmas generales, responsabilidad de los proveedores del servicio de red, contratos electrónicos, registros electrónicos seguros y firmas, los efectos de firmas digitales, obligaciones generales con relación a la firma digital, obligaciones de las autoridades certificadoras, obligaciones de suscriptores, regulación de autoridades certificadoras, uso de registros y firmas electrónicas del gobierno y, por último, disposiciones generales.

Por su parte, el Reglamento de Transacciones Electrónicas (*Electronic Transactions [Certification Authority] Regulation*) de 1999, consta de un total de ocho partes que se refieren a la expedición de

licencias de autoridades certificadoras, criterios para su expedición y revocación, conducta empresarial de las autoridades certificadoras licenciadas, requisitos para los repositorios, solicitudes al gobierno y otras corporaciones legales y normas administrativas.

El punto que me interesa aquí se encuentra en el art. 2º de la ley que se refiere a las autoridades certificadoras, al concepto de certificado y a la autoridad controladora, en los siguientes términos:

Certificado. Significa un registro expedido con el propósito de avalar firmar digitales, el cual pretende confirmar la identidad u otras características importantes de la persona que posee una clave de llaves particular.

Autoridad Certificadora. La persona física o moral que expide un certificado.

Controladora. Alude al organismo regulador de autoridades de certificación previsto en la sección 41 (1) y la cual incluye un representante o un asistente previstos en la sección 41 (2).²

El art. 3º del Reglamento es el que se refiere a la solicitud para la licencia respectiva, en los términos siguientes:

§ 3. Solicitud de licencia de las autoridades de certificación.

1. Toda solicitud para convertirse en una autoridad de certificación licenciada debe ser hecha en la forma y en los términos como lo determine la autoridad Controladora, según se requiera y debe estar apoyada en la documentación que esta misma autoridad exija.

2. La autoridad Controladora puede exigir al solicitante que proporcione la información adicional necesaria en apoyo de su solicitud.

3. La autoridad Controladora puede recibir solicitudes para la renovación de licencias que consten en la forma de registro electrónicos. En este caso, se someterán a los requisitos que dicha autoridad exija.

4. La licencia debe estar sujeta a las condiciones, restricciones y limitaciones que la autoridad controladora deba exigir, según las condiciones del caso.³

² “§ 2. Interpretation.

Certificate. Means a record issued for the purpose of supporting digital signatures which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;

Certification authority. Means a person who or an organization that issues a certificate;

Controller. Means the Controller of Certification Authorities appointed under section 41(1) and includes a Deputy or an Assistant Controller of Certification Authorities appointed under section 41(2).”

³ “§ 3. Application to be licensed certification authority.

La Parte Décima del ETA es muy importante, porque se refiere exclusivamente en sus arts. 41-46 a la regulación de las autoridades certificadoras (*certification authorities*). Así, se designa especialmente una Autoridad Controladora (*Controller of Certification Authorities*) que tiene la obligación de expedir las licencias y la supervisión y vigilancia de las autoridades certificadoras, en estrecha relación con el ministerio del ramo. A su vez, las obligaciones de las autoridades de certificación se resumen principalmente en la expedición de un certificado de procedimientos (*certification practice statements*) que contiene la información técnica relativa que la propia autoridad de certificación emplea en la expedición de los certificados. Es importante aclarar que el art. 43 señala en forma expresa cuáles son los requerimientos que deben reunir las autoridades certificadoras extranjeras.

§ 43. Reconocimiento de autoridades de certificación extranjeras.

- a) El límite de confiabilidad recomendado, si lo hay, especificado en un certificado expedido por la autoridad de certificación.
- b) La presunción que ha sido referida en las secciones 20(b)(ii) y 21.⁴

Este último inciso b) hace referencia a las firmas digitales seguras y confiables avaladas por autoridades extranjeras, así como a la presunción, a menos de evidencia en contrario, de que la información que aparece en un certificado es correcta, si este certificado fue aceptado por el suscriptor.

El periodo de validez de esta licencia es de un año, a criterio de la autoridad controladora (*Controller of Certification Authorities [CCA]*), la cual a su vez depende de la *National Computer Board*, a cargo de *The International Trade Security Office*.

1. Every application to be a licensed certification authority shall be made in such form and manner as the Controller may, from time to time, determine and shall be supported by such information as the Controller may require.

2. The Controller may require the applicant to furnish such additional information as are necessary in support of the application.

3. The Controller may allow applications for renewal of licenses to be submitted in the form of electronic records subject to such requirements as the Controller may impose.

4. A license shall be subject to such conditions, restrictions and limitations as the Controller may, from time to time, determine.”

⁴ “§ 43. Recognition of foreign certification authorities.

a) the recommended reliance limit, if any, specified in a certificate issued by the certification authority;

b) the presumption referred to in sections 20(b)(ii) and 21.”

Las tarifas ascienden a la cantidad de \$5,000 dólares, más una tasa anual de \$1,000 dólares.

Por su parte, los arts. 7º y 8º de la ley establecen los criterios para la expedición de las licencias. Son los siguientes:

§ 7. Criterios de financiación.

1. Una solicitud para la expedición de licencias debe satisfacer los criterios siguientes:

- a) El solicitante debe ser una compañía que opere en Singapur;
- b) El solicitante debe estar asegurado en contra de la responsabilidad por pérdidas no menores de \$1 millón por cada reclamación instaurada en virtud de error u omisión de parte del solicitante, sus funcionarios o empleados;
- c) El solicitante debe tener:
 - i) No menos de \$2 millones de capital pagado; y
 - ii) Además, un capital pagado combinado y la prueba de financiación disponible por no menos de cinco millones, y
 - d) El solicitante debe obtener una garantía de ejecución o garantía bancaria a favor de la autoridad Controladora en los términos aprobados por esta misma, por una cantidad no menor de un millón.

2. La fianza o garantía bancaria referida en el parágrafo (1) (d) puede ser invocada:

- a) Para el pago de una oferta o convenio hecho por la autoridad controladora;
- b) Para el pago de responsabilidad y costos de rectificación imputables a la negligencia de la autoridad certificadora, de sus funcionarios o empleados; o
- c) Para el pago de los costos en que se incurra a causa de la cesación o transferencia de operaciones de la autoridad de certificación licenciada, si es el caso.

§ 8. Personal.

1. El solicitante debe adoptar medidas razonables para garantizar que cada persona certificada:

- a) Es la persona adecuada para responder de las obligaciones asignadas;
- b) No se trata de una empresa en quiebra en Singapur o en alguna otra parte o se encuentre efectuando convenios o arreglos con acreedores; y
- c) Que no haya sido sentenciada, ya sea en Singapur o en alguna otra parte, respecto de:
 - i) Un delito de carácter patrimonial; o
 - ii) Un delito objeto de esta ley o de su reglamento.⁵

⁵ "§ 7. Financial criteria, etc.

Además, el ETR exige que la persona a quien se expida la licencia de autoridad certificadora debe tener un adecuado conocimiento de la Ley y del Reglamento, tener capacitación técnica en la expedición de este tipo de certificados y poseer, además, la suficiente experiencia para cumplir con las obligaciones respectivas.

El ETR establece con mucho detalle, en su art. 11, las circunstancias en virtud de las cuales puede negarse la expedición o renovación de la licencia. Estas causas comprenden la falta de información necesaria a la autoridad controladora, con respecto a sus funcionarios o a su conducta negocial, vicisitudes diversas en la marcha económica de la compañía, compromisos con acreedores, antecedentes delictivos de las personas, deshonestidad en general, ausencia de respaldo financiero, antecedentes de ineficiencia de parte de la compañía y, por último, hasta una causa sumamente

1. An applicant for a license shall comply with the following criteria:
a) the applicant must be a company operating in Singapore;
b) the applicant must be insured against liability for loss of not less than \$1 million for each claim arising out of any error or omission on the part of the applicant, its officers or employees;
c) the applicant must have:
i) not less than \$2 million in paid-up capital; and
ii) in addition, a combined paid-up capital and proof of available financing of not less than \$5 million; and
d) the applicant must obtain a performance bond or banker's guarantee in favour of the Controller in a form approved by the Controller for an amount of not less than \$1 million.

2. The performance bond or banker's guarantee referred to in paragraph (1)(d) may be invoked:

a) for payment of an offer of composition made by the Controller;
b) for payment of liabilities and rectification costs attributed to the negligence of the certification authority, its officers or employees; or
c) for payment of the costs incurred in the discontinuation or transfer of operations of the licensed certification authority, if the certification authority's license or operations is discontinued."

"§ 8. Personnel.

1. An applicant shall take reasonable measures to ensure that every trusted person:
a) is a fit and proper person to carry out the duties assigned to him;
b) is not an undercharged bankrupt in Singapore or elsewhere or has made a composition or an arrangement with his creditors; and
c) has not been convicted, whether in Singapore or elsewhere, of:
i) an offence the conviction for which involved a finding that he acted fraudulently or dishonestly; or
ii) an offence under the Act or these Regulations."

Sin embargo, es importante advertir en este punto que, si bien se establece como requisito la ausencia de antecedentes penales, también es cierto que puede excepcionalmente permitirse su ingreso si el solicitante demuestra ser una persona actualmente honorable y si han transcurrido diez años desde la fecha de la sentencia o su liberación, en el caso de sanción privativa de libertad (lo que más le favorezca).

discrecional que alude al hecho de que la autoridad controladora opine que resulta “en interés del público hacerlo”.⁶

El capítulo 4º del ETR y los arts. 11-15 de la ETA se refieren precisamente a los contratos electrónicos.⁷ La Parte Quinta, en

⁶ He aquí el texto íntegro de este importante artículo:

“§ 11. Controller to refuse to grant or renew licenses in certain circumstances

1. The Controller may refuse to grant or renew a license if:

a) the applicant has not provided the Controller with such information relating to it or any person employed by or associated with it for the purposes of its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require;

b) the applicant or its substantial shareholder is in the course of being wound up or liquidated;

c) a receiver or a receiver and manager has been appointed to the applicant or its substantial shareholder;

d) the applicant or its substantial shareholder has, whether in Singapore or elsewhere, entered into a compromise or scheme of arrangement with its creditors, being a compromise or scheme of arrangement that is still in operation;

e) the applicant or its substantial shareholder or any trusted person has been convicted, whether in Singapore or elsewhere, of an offence the conviction for which involved a finding that it or he acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these Regulations;

f) the Controller is not satisfied as to the qualifications or experience of the trusted person who is to perform duties in connection with the holding of the license by the applicant;

g) the applicant fails to satisfy the Controller that it is a fit and proper person to be licensed or that all its trusted persons and substantial shareholders are fit and proper persons;

h) the Controller has reason to believe that the applicant may not be able to act in the best interest of its subscribers, customers or participants having regard to the reputation, character, financial integrity and reliability of the applicant or any of its substantial shareholders or trusted persons;

i) the Controller is not satisfied as to the financial standing of the applicant or its substantial shareholder;

j) the Controller is not satisfied as to the record of past performance or expertise of the applicant or its trusted person having regard to the nature of the business which the applicant may carry on in connection with the holding of the license;

h) there are other circumstances which are likely to lead to the improper conduct of business by, or reflect discredit on the method of conducting the business of, the applicant or its substantial shareholder or any of the trusted persons; or

1. the Controller is of the opinion that it is in the interest of the public to do so.”

⁷ Es importante tener presente aquí el sentido del art. 4 del ETA que especifica claramente cuáles son los negocios jurídicos a los que no es posible aplicar, en términos de esta ley, los principios de la contratación electrónica. Estos negocios jurídicos comprenden el testamento, los títulos de crédito, escrituras, poderes de representación, transferencia de bienes inmuebles, garantías sobre los mismos, etc. Este es el texto íntegro del parágrafo:

“§4. Application.

(1) Parts II and IV shall not apply to any rule of law requiring writing or signatures in any of the following matters:

a) the creation or execution of a will;

b) negotiable instruments;

cambio, se refiere nuevamente a la conducta empresarial por las autoridades certificadoras que posean la licencia respectiva. Así, se establece en el art. 16 que estas autoridades pueden mantener sus propios registros ya sea en soporte papel, en soporte electrónico o en cualquier otra forma aprobada por la Controladora. Estos registros deben ser clasificados, almacenados, preservados y reproducidos de forma tal que todo el proceso pueda ser verificado por la Controladora, por auditores o por funcionarios competentes. Se establece expresamente la obligación de guardar los registros por un plazo no menor a siete años.

Los artículos siguientes establecen reglas específicas que atañen a los distintos tipos de licencias, así como al procedimiento de expedición de los mismos, suspensión, revocación y expiración.⁸ De todas formas es importante advertir en este último punto que el art. 23 es contundente —y lacónico— al advertir que el certificado debe establecer expresamente la fecha de su vigencia.⁹

Probablemente uno de los puntos más importantes de este Reglamento en Singapur se refiere a los requisitos técnicos de seguridad electrónica, lo cual debe confrontarse con lo dispuesto en los arts. 16-18 de la ETA. Así, los arts. 25-29 establecen en forma detallada los procedimientos de seguridad y verificación digital al respecto. Es importante incluso aclarar que tales procedimientos deben estar rigurosamente publicados en un sitio de la red (*Controller's Internet website*) bajo la supervisión constante de la autoridad controladora. Además, cada autoridad certificadora regulada en términos de este ETR debe asegurar la provisión a cada suscriptor de un sistema confiable para generar su propio par de llaves, así como los mecanismos que comprueben la validez de la firma y el estatus del certificado. La autoridad certificadora es responsable del almacenamiento de las llaves.

c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;

d) any contract for the sale or other disposition of immovable property, or any interest in such property;

e) the conveyance of immovable property or the transfer of any interest in immovable property.

f) Documents of title.

(2) The Minister may by order modify the provisions of subsection (1) by adding, deleting or amending any class of transactions or matters.”

⁸ Este procedimiento, previsto en el art. 19, también es aplicable para la renovación del documento. *Cfr.* arts. 29, 31, 32-35 del ETA.

⁹ “§ 23. Expiry date of certificates.

A certificate must state the date on which it expires.”

Dada la estrecha relación existente entre las autoridades certificadora y controladora, se establece en el art. 29 la obligación de aquélla para informar a esta última de cualquier cambio en el nombramiento de sus autoridades internas o de cualquier persona que ejecute funciones equivalentes a las mismas, dentro del plazo de tres días hábiles a partir de la asunción del cargo.¹⁰

Conviene ahora, finalmente, examinar lo relativo a la obligación de las autoridades certificadoras para reportar periódicamente la naturaleza y extensión de sus actividades y el reporte financiero correspondiente. Así, el art. 34.1 exige el envío de este informe cada seis meses. Este reporte debe incluir la información necesaria que se refiera a los reportes financieros, número de suscriptores, número de certificados expedidos, suspendidos, revocados, terminados y renegociados, cambios estructurales y datos personales de los funcionarios. Es también importante advertir que toda esta información debe ser publicada en el sitio *web* de la autoridad de certificación licenciada.¹¹

Esta información comprende también, por cierto, la noticia acerca de la continuación de actividades por parte de la autoridad certificadora, puesto que tiene la obligación de anticipar, con un mínimo de tres meses, la intención de suspender sus operaciones

¹⁰ "§ 29. Change in management.

A licensed certification authority shall inform the Controller of any changes in the appointment of any person as its director or chief executive, or of any person to perform functions equivalent to that of a chief executive, within 3 working days from the date of appointment of that person."

¹¹ "§ 34. Disclosure.

1. The licensed certification authority must submit half-yearly progress and financial reports to the Controller.

2. The half-yearly progress reports must include information on:

a) the number of subscribers;
b) the number of certificates issued, suspended, revoked, expired and renewed;
c) system performance including system up and down time and any extraordinary incidents;
d) changes in the organizational structure of the certification authority;
e) changes since the preceding progress report submitted or since the application for the license, and

f) changes in the particulars of any trusted person since the last submission to the Controller, including the name, identification number, residential address, designation, function and date of employment of the trusted person.

3. The licensed certification authority has a continuing obligation to disclose to the Controller any changes in the information submitted.

4. All current versions of the licensed certification authority's applicable certification practice statements together with their effective dates must be published in the licensed certification authority's Internet website."

con el correspondiente aviso tanto a suscriptores como al público en general.

Por último, los arts. 48 (2) y 56 de la Ley y 36 y 37 del ETR se ocupan de las sanciones especificando la protección de la obligación de confiabilidad, con penas que no deben exceder de ciertas cantidades o con pena de prisión —o ambas en su caso—. ¹²

3. LEY 527 POR MEDIO DE LA CUAL SE DEFINE Y REGLAMENTA EL ACCESO Y USO DE LOS MENSAJES DE DATOS, DEL COMERCIO ELECTRÓNICO Y DE LAS FIRMAS DIGITALES, Y SE ESTABLECEN LAS ENTIDADES DE CERTIFICACIÓN Y SE DICTAN OTRAS DISPOSICIONES, COLOMBIA, 1999

Esta ley define el concepto *entidad de certificación* en la siguiente forma:

ART. 2º—Definiciones.

...

d) Entidad de certificación. Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;...

La Parte Tercera de esta ley se dedica a las firmas digitales, a los certificados y Entidades de Certificación (EC). Conforme a lo dispuesto en el art. 29, las características y requerimientos de las entidades de certificación son en primer lugar, que se trate de

¹² “§ 48. (ETA) Obligation of confidentiality.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 12 months or to both.”

“§56. (ETA) General penalties.

Any person guilty of an offence under this Act or any regulations made there under for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 6 months or to both.”

“§ 36. (ETR) Penalties.

Any person who fails, without any reasonable excuse, to comply with regulation 16(2), 17, 19(2) or (11), 20(3), 21(10), 22(5), 24(7) or (8) or 28 shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$5,000 and, in the case of a second or subsequent conviction, to a fine not exceeding \$10,000.”

“§ 37. (ETR) Composition of offences.

Any offence under these Regulations may be compounded by the Controller under section 59 of the Act.”

personas jurídicas, ya sea de naturaleza pública o privada, no importando si son de origen nacional o extranjero. Se prevé especialmente el caso de las cámaras de comercio. Sus requisitos más importantes son los siguientes:

- a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación;
- b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley;
- c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

Estas entidades de certificación deberán estar autorizadas por la Superintendencia de Industria y Comercio. Esta oficina tendrá las siguientes facultades:

ART. 41.—Funciones de la Superintendencia...

1. Autorizar la actividad de las entidades de certificación en el territorio nacional.
2. Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación.
3. Realizar visitas de auditoría a las entidades de certificación.
4. Revocar o suspender la autorización para operar como entidad de certificación.
5. Solicitar la información pertinente para el ejercicio de sus funciones.
6. Imponer sanciones a las entidades de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.
7. Ordenar la revocación de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.
8. Designar los repositorios y entidades de certificación en los eventos previstos en la ley.
9. Emitir certificados en relación con las firmas digitales de las entidades de certificación.
10. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación.

11. Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.

Sus obligaciones se reducen a las siguientes:

ART. 30.—Actividades de las entidades de certificación...

1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.
2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.
3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales *f*) y *g*) del artículo 26 de la presente ley.
4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.
5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.
6. Ofrecer los servicios de archivo y conservación de mensajes de datos.

Es importante aclarar que la remuneración de los servicios de la EC serán establecidos libremente por cada una de las entidades, quienes, en contraprestación, deberán cumplir con las siguientes obligaciones:

ART. 32.—Deberes de las entidades de certificación...

- a*) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;
- b*) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;
- c*) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;
- d*) Garantizar la prestación permanente del servicio de entidad de certificación;
- e*) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;
- f*) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley;
- g*) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;

- h) Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio;
- i) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio;
- j) Llevar un registro de los certificados.

A su vez, el certificado emitido por la EC deberá contener los siguientes datos:

ART. 35.—Contenido de los certificados:

1. Nombre, dirección y domicilio del suscriptor.
2. Identificación del suscriptor nombrado en el certificado.
3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
4. La clave pública del usuario.
5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
6. El número de serie del certificado.
7. Fecha de emisión y expiración del certificado.

Los artículos siguientes consigan normas específicas sobre aceptación y revocación de los certificados.

Por cuanto hace a sanciones, éstas se hacen consistir en amonestación, multas en lo económico del orden de hasta dos mil salarios mínimos legales mensuales vigentes, suspensión, prohibición de prestación de servicios hasta por cinco años y revocación definitiva de la autorización.

Se establece expresamente que los certificados de firmas digitales emitidos por entidades de certificación extranjeras podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley, como si fueran nacionales. Sin embargo, se añade el requisito de que tales certificados sean reconocidos por una entidad de certificación autorizada que regule todo el procedimiento.

Por último, interesa destacar que esta Superintendencia de Industria y Comercio tiene facultades expresas, conforme a lo dispuesto por el art. 41.8, para designar los repositorios y entidades de certificación en los casos previstos en la ley. No se establece vigencia alguna de los certificados, aunque en un proyecto anterior del año de 1998 se establecía (en un art. 41 que luego no aparece ya en la ley) que “Un certificado emitido por una entidad de certificación expira en la fecha indicada en el mismo. Sin em-

bargo, la fecha de expiración de un certificado en ningún caso podrá ser superior a un (1) año”.

También en este mismo proyecto se establecía en el art. 47 la conservación de los registros de certificados expedidos por un término de cuarenta años, a cargo de la propia entidad de certificación. Sin embargo, en la ley vigente el art. 38 solamente establece que tales registros deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular.

Tampoco aparece en la ley, por último, el capítulo VI que se dedicaba a los repositorios y cuyo comentario se reduce ahora únicamente a lo dispuesto en el art. 41.8 de la ley.

4. PROYECTO DE LEY SOBRE DOCUMENTOS ELECTRÓNICOS, CHILE

Este proyecto consigna las siguientes definiciones:

ART. 2º—Para todos los efectos legales se entenderá por:

...

2º Archivos o registros electrónicos: Toda información archivada por medios electrónicos, ópticos u otros análogos.

3º Autenticación: Medio o procedimiento a través de la cual es posible verificar la identidad de un originador o destinatario de documentos electrónicos.

4º Certificación Electrónica: Procedimiento informático en virtud del cual la autoridad certificadora genera un código único e inalterable, adjunto a la llave pública de una persona natural o jurídica, cuya función es garantizar que los datos contenidos en la llave están vigentes, son auténticos, están inalterados y corresponden a dicha persona natural.

...

11º Intermediario o red de valor agregado: Persona natural o jurídica que, en representación o por cuenta de otra persona natural o jurídica, recibe, transmite o archiva documentos electrónicos o provee otros servicios respecto de tales documentos.

15º Sello Electrónico: Firma digital o electrónica de una persona jurídica que permite garantizar la integridad de un documento electrónico y que, adicionalmente, permite garantizar su confidencialidad mediante la criptografía.

Es muy importante destacar en este proyecto que la parte final del art. 4º que se refiere a los requisitos de la firma electrónica consigna claramente que “... Lo dispuesto en este artículo será aplicable al endoso de documentos mercantiles, tales como factu-

ras, letras de cambio, pagarés, pólizas de seguro, documentos de embarque y cualquier otro documento que sea representativo de valores transables”, lo cual representa desde luego una importante novedad en la inclusión de los negocios susceptibles de manejo electrónico (*Cj.*: art. 4º ETA, Singapur).

Otra novedad reside en los arts. 7-11 y 30-31 que involucran la participación de los denominados “ministros de fe”. En este proyecto original se reguló originalmente la equiparación del documento electrónico con la formalidad de una escritura pública, a través de la utilización de firmas electrónicas y la imposición de un sello asimismo electrónico. También se preveía la creación del protocolo notarial electrónico, junto con un repertorio y un índice público.

Ahora bien, con fecha 10 de junio de 1999 se dictó el “Decreto que regula el uso de la firma digital y los documentos electrónicos en la administración del Estado”. Así, el art. 1º dice:

ART. 1º—El presente decreto tiene por objeto regular la utilización de la firma digital y los documentos electrónicos como soporte alternativo a la instrumentalización en papel de las actuaciones de los órganos de la Administración del Estado. También establece las condiciones en que los datos contenidos en un soporte electrónico se considerarán emanados de una persona determinada.

Las normas de este decreto sólo serán aplicables a los órganos de la Administración del Estado mencionados en el artículo 1º de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, con la salvedad de la Contraloría General de la República, el Banco Central y las municipalidades. Sin embargo, dichos órganos podrán acogerse voluntariamente a las normas de este decreto, mediante una comunicación escrita en tal sentido, dirigida al Ministerio Secretaría General de la Presidencia.

Este Decreto contiene las siguientes definiciones:

ART. 2º—Para los efectos de este decreto se entenderá por:

a) Documento electrónico: Toda representación informática que da testimonio de un hecho.

...

g) Certificado de firma digital: Documento electrónico emitido por el ministro de fe del servicio respectivo que acredita la correspondencia entre una clave pública y la persona que es titular de la misma.

Por otra parte, se distinguen con mucha claridad los conceptos de firma electrónica y firma digital en la siguiente forma:

...

b) Firma electrónica: Código informático que permite determinar la autenticidad de un documento electrónico y su integridad, impidiendo a su transmisor desconocer la autoría del mensaje en forma posterior.

c) Firma digital: Especie de firma electrónica que resulta de un proceso informático validado, implementado a través de un sistema criptográfico de claves públicas y privadas.

Asimismo, se toman en cuenta cuatro puntos importantes para la utilización de los soportes, medios y aplicaciones electrónicas en las actuaciones administrativas. Se reducen a los siguientes:

- a) Autenticidad;
- b) Confidencialidad;
- c) Integridad, y
- d) Conservación.

El art. 4º reproduce, por cierto, los mismos términos de la ley italiana al indicar que:

Los documentos de los órganos señalados en el artículo 1º escritos en un soporte electrónico, producirán los mismos efectos que los escritos en un soporte de papel.

En dichos documentos, la firma digital sustituirá a la firma ológrafa del funcionario que lo emite y producirá los mismos efectos que aquella. En consecuencia, cuando un documento electrónico sea firmado digitalmente, se entenderá que emana del funcionario titular de dicha firma digital y producirá los mismos efectos jurídicos que el documento escrito y firmado ológrafamente en soporte de papel.

La firma digital sustituirá el uso de cualquier sello, timbre, visto bueno u otra marca distinta que fuere necesaria para la validez del documento, si éste hubiere sido escrito sobre un soporte de papel.

Por su parte, el art. 5º dice que:

Los documentos electrónicos firmados digitalmente que deban ser publicados o notificados a un particular, deberán ser traspasados a soporte papel. Su correspondencia con el original electrónico será certificada por el respectivo ministro de fe. En lo demás, seguirán las reglas generales de dichos documentos.

Se dice especialmente respecto de las copias autorizadas que tendrán este carácter siempre que el ministro de fe del servicio acredite su correspondencia con el documento electrónico firma-

do digitalmente. En este caso, el ministro de fe debe imponer a la copia su firma ológrafa conforme a las reglas generales.

Es importante mencionar que la suspensión o revocación de una clave pública solamente comienza a producir efectos legales hasta que haya sido registrada por el respectivo ministro de fe (art. 9º).

El organismo regulador de todo el servicio es el Ministerio Secretaría General de la Presidencia.

5. DECRETO 427/98 DE FIRMAS DIGITALES PARA LA ADMINISTRACIÓN PÚBLICA NACIONAL, ARGENTINA, 1998

Es importante aclarar que este decreto, como su nombre lo advierte, se reduce exclusivamente a la administración pública nacional y, por tanto, no produce efectos jurídicos individuales en forma directa, aunque de todas formas, el ámbito de aplicación es sumamente amplio porque comprende todo el sector público nacional:

Las disposiciones del presente Decreto serán de aplicación en todo el ámbito del Sector Público Nacional, dentro del cual se comprende la administración centralizada y la descentralizada, los entes autárquicos, las empresas del Estado, Sociedades del Estado, Sociedades Anónimas con participación estatal mayoritaria, los bancos y entidades financieras oficiales y todo otro ente, cualquiera que sea su denominación o naturaleza jurídica, en que el Estado Nacional o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones. (Art. 3º.)

Se establece en este decreto que la supervisión y control, como organismo licenciante, corresponde a la Secretaría de la Función Pública de las Jefaturas de Gabinetes de Ministros, con el auxilio de la Contaduría General de la Nación dependiente de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del Ministerio de Economía y Obras y Servicios Públicos, como organismo auditante.

El anexo I de este decreto 427/98 se refiere específicamente a la infraestructura de firma digital en el mismo ámbito. Así, el organismo licenciante dispone de las siguientes funciones:

1. Otorga las licencias habilitantes para acreditar a las autoridades certificadoras y emite los correspondientes *certificados de clave pública*, que permiten *verificar las firmas digitales* de los *certificados* que éstas emitan;
2. Deniega las solicitudes de licencias a las autoridades certificadoras que no cumplan con los requisitos establecidos para su autorización;

3. Revoca las licencias otorgadas a las *Autoridades Certificantes Licenciadas* que dejan de cumplir con los requisitos establecidos para su autorización;
4. Verifica que las *Autoridades Certificantes Licenciadas* utilicen sistemas *técnicamente confiables*;
5. Considera para su aprobación el manual de procedimientos, el plan de seguridad y el de cese de actividades presentados por las autoridades certificadoras;
6. Acuerda con el *organismo auditante* el plan de auditoría para las *Autoridades Certificantes Licenciadas*;
7. Dispone la realización de auditorías de oficio;
8. Resuelve los conflictos individuales que se susciten entre el *suscriptor* de un *certificado* y la *autoridad certificante licenciada* emisora del mismo, y
9. Resuelve todas aquellas contingencias respecto a la infraestructura de *firma digital*.

A su vez, tendrá las siguientes obligaciones:

En su calidad de *suscriptor* de *certificado* y de autoridad certificante, el *organismo licenciante* tiene idénticas obligaciones que las *Autoridades Certificantes Licenciadas*, y además debe:

1. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la *clave privada* de cualquier *suscriptor* de los *certificados* que emita;
2. Mantener el control de su propia *clave privada* e impedir su divulgación;
3. Revocar su propio *certificado de clave pública* frente al compromiso de su *clave privada*;
4. Permitir el acceso público permanente a los *certificados de clave pública* que ha emitido en favor de las *Autoridades Certificantes Licenciadas*, y a la *lista de certificados revocados*, por medio de conexiones de telecomunicaciones públicamente accesibles. Esto también se aplica a la información sobre direcciones y números telefónicos de las *Autoridades Certificantes Licenciadas*;
5. Permitir el ingreso de los funcionarios autorizados del *organismo auditante* a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso;
6. Publicar su propio *certificado de clave pública* en el Boletín Oficial, y en *dos* (2) diarios de difusión nacional, durante *tres* (3) días consecutivos a partir del día de su emisión;
7. Revocar los *certificados* emitidos en favor de las *Autoridades Certificantes Licenciadas* incursas en causales de revocación de licencia, o que han cesado sus actividades;

8. Revocar los *certificados* emitidos en favor de las *Autoridades Certificantes Licenciadas*, cuando las *claves públicas* que en ellos figuran dejan de ser *técnicamente confiables*;
9. Supervisar la ejecución del plan de cese de actividades de las *Autoridades Certificantes Licenciadas* que discontinúan sus funciones;
10. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

Por otra parte, la Autoridad Certificadora Licenciada tendrá las siguientes funciones:

1. Emite *certificados de clave pública*;
Para emitir *certificados de clave pública*, la *autoridad certificante licenciada* debe:
 - a) Recibir del agente requirente una solicitud de *emisión de certificado de clave pública*, la cual deberá estar firmada digitalmente con la correspondiente *clave privada*;
 - b) Verificar fehacientemente la información identificatoria del solicitante, la cual deberá estar siempre incluida en el *certificado*, y toda otra información que según lo dispuesto en el manual de procedimientos de la *autoridad certificante licenciada*, deba ser objeto de verificación, lo cual deberá realizarse de acuerdo a lo dispuesto en el citado manual;
 - c) Numerar correlativamente los *certificados emitidos*;
 - d) Mantener copia de todos los *certificados* emitidos, consignando su fecha de emisión.

La *Autoridad Certificante Licenciada* puede, opcionalmente, incluir en un *certificado* información no verificada, debiendo indicar claramente tal cualidad.

2. Revoca *certificados de clave pública*;
La *autoridad certificante licenciada* revocará los *certificados de clave pública* por ella emitidos:
 - a) por solicitud de su *suscriptor*; o
 - b) por solicitud de un *tercero*; o
 - c) si llegara a determinar que un *certificado* fue emitido en base a una información falsa, que en el momento de la *emisión* hubiera sido objeto de verificación; o
 - d) si llegara a determinar que las *claves públicas* contenidas en los *certificados* dejan de ser *técnicamente confiables*; o
 - e) si cesa en sus actividades y no transfiere los *certificados* emitidos por ella a otra *autoridad certificante licenciada*;

La solicitud de *revocación de un certificado* debe hacerse en forma personal o por medio de un *documento digital firmado*. Si la revocación

es solicitada por el *suscriptor*, ésta deberá concretarse de inmediato. Si la revocación es solicitada por un *tercero*, tendrá lugar dentro de los plazos mínimos necesarios para realizar las verificaciones del caso. La revocación debe indicar el momento desde el cual se aplica y no puede ser retroactiva o a futuro. El *certificado* revocado deberá incluirse inmediatamente en la *lista de certificados revocados*, y la lista debe estar firmada por la *Autoridad Certificante Licenciada*. Dicha lista debe hacerse pública en forma permanente, por medio de conexiones de telecomunicaciones públicamente accesibles.

La *Autoridad Certificante Licenciada* debe emitir una constancia de la revocación para el solicitante.

3. Provee, opcionalmente, el servicio de *sellado digital de fecha y hora*.

Sus obligaciones se reducen a las siguientes:

Adicionalmente a sus obligaciones emergentes como *suscriptora* de su *certificado* emitido por el *organismo licenciante*, la *autoridad certificante licenciada* debe:

1. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la *clave privada* del *suscriptor*;
2. Mantener el control de su *clave privada* e impedir su divulgación;
3. Solicitar inmediatamente la *revocación de su certificado*, cuando tuviera sospechas fundadas de que su *clave privada* ha sido comprometida;
4. Solicitar al *organismo licenciante* la revocación de su *certificado* cuando la *clave pública* en él contenida deje de ser *técnicamente confiable*;
5. Informar inmediatamente al *organismo licenciante* sobre cualquier cambio en los datos contenidos en su *certificado*, o sobre cualquier hecho significativo que pueda afectar la información contenida en el mismo;
6. Operar utilizando un sistema *técnicamente confiable*;
7. Notificar al solicitante sobre las medidas necesarias que éste está obligado a adoptar para crear *firmas digitales* seguras y para su *verificación* confiable; y de las obligaciones que éste asume por el solo hecho de ser *suscriptor* de un *certificado de clave pública*;
8. Recabar únicamente aquellos datos personales del *suscriptor* del *certificado* que sean necesarios y de utilidad para la emisión del mismo, quedando el solicitante en libertad de proveer información adicional. Toda información así recabada, pero que no figure en el *certificado*, será de trato confidencial por parte de la *autoridad certificante licenciada*;
9. Poner a disposición del *suscriptor* de un *certificado* emitido por esta *autoridad certificante licenciada*, toda la información relativa a la tramitación del *certificado*;

10. Mantener la documentación respaldatoria de los *certificados* emitidos por diez (10) años a partir de su fecha de vencimiento o revocación;
11. Permitir el acceso público permanente a los *certificados* que ha emitido, y a la *lista de certificados revocados*, por medio de conexiones de telecomunicaciones públicamente accesibles;
12. Publicar su dirección y sus números telefónicos;
13. Permitir el ingreso de los funcionarios autorizados del *organismo licenciante* o del *organismo auditante* a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso;
14. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

Se establecen también las condiciones para el cese de actividades de una autoridad certificadora licenciada, así como las obligaciones del suscriptor de certificado de clave pública.

Estos certificados de clave pública tendrán el siguiente contenido:

El *certificado de clave pública* contendrá, como mínimo, los siguientes datos:

1. Nombre del *suscriptor del certificado*;
2. Tipo y número de documento del *suscriptor del certificado*, o número de licencia, en el caso de *certificados* emitidos para *autoridades certificadoras licenciadas*;
3. *Clave pública* utilizada por el *suscriptor*;
4. Nombre del algoritmo que debe utilizarse con la *clave pública* en él contenida;
5. Número de serie del *certificado*;
6. *Periodo de vigencia del certificado*;
7. Nombre de la *Autoridad Certificante Licenciada* emisora del *certificado*;
8. *Firma digital* de la *Autoridad Certificante Licenciada* que emite el *certificado*, identificando los algoritmos utilizados;
9. Todo otro dato relevante para la utilización del *certificado*, se explicitará en el manual de procedimientos de la *Autoridad Certificante Licenciada* emisora.

Probablemente por la condición de uso interno en el ámbito de la administración pública nacional, ni el decreto ni los anexos establecen costos. De conformidad con lo dispuesto en el “Anexo Uno”, el certificado de clave pública debe establecer expresamente su periodo de vigencia.

6. LEY DE FIRMAS Y CERTIFICADOS DIGITALES, PERÚ

En la ley peruana se define el *certificado digital* en términos de lo dispuesto en el art. 6º como "... el documento electrónico generado y firmado digitalmente por una entidad de certificación la cual vincula un par de claves con una persona determinada confirmando su identidad".

Este certificado digital deberá contener los siguientes datos:

1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación. (Art. 7º.)

Se establecen normas expresas que protegen la confidencialidad de la información, la cancelación del certificado y la revocación del mismo.

Veamos ahora lo relativo a las entidades de certificación y su registro. Conforme a lo dispuesto por el art. 12:

La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general.

Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o de Verificación.

A su vez, la Entidad de Registro o de Verificación tiene la función de:

Levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital, aceptación y autorización de solicitudes de emisión de certificados digitales, aceptación y autorización de las solicitudes de cancelación de certificados digitales. (Art. 13.)

Las Entidades de Certificación deben llevar un registro permanente donde consten todos los certificados digitales que hayan sido

emitidos. Además, este registro debe ser accesible por medios telemáticos y será público.

Tanto las Entidades de Certificación cuanto la Entidad de Registro o de Verificación estarán sujetas a la vigilancia y control del poder ejecutivo. Esta ley no consigna qué tipo de vigilancia, lo que probablemente será materia del reglamento que en su oportunidad se dicte.

Por último, el art. 11 se refiere al reconocimiento de certificados emitidos por entidades extranjeras en los siguientes términos:

Los Certificados de Firmas Digitales emitidos por Entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por una Entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos del procedimiento así como la validez y la vigencia del certificado.

Probablemente la figura que más llama la atención en la legislación peruana es la que se refiere al “Fedatario Particular Juramentado en Informática”. El 11 de octubre de 1991 se dictó el decreto legislativo N° 681, publicado apenas tres días después. En virtud de este decreto se establecían como figuras centrales de la contratación electrónica al notario público y a este “Fedatario Particular Juramentado en Informática”.

En términos de lo dispuesto en el art. 3° del decreto legislativo en análisis, este especial fedatario adquiere la categoría de funcionario: “... se consideran depositarios de la fe pública y mantienen en todo momento su independencia de las empresas a las que ofrecen sus servicios”. Pueden funcionar adscritos a una notaría pública, en cuyo caso cobran el carácter de “Fedatarios Públicos Juramentados”.

El requisito importante para acceder a esta calidad sería la obtención de un “diploma de idoneidad técnica”, que se expediría al final de una capacitación específica. Desde luego, se exige que este fedatario juramentado sea un abogado de carrera, pero al mismo tiempo se busca que tenga conocimientos de informática para el mejor cumplimiento de su labor. Corresponde a los colegios de abogados y de notarios la expedición del correspondiente certificado, con la previa impartición de los cursos respectivos.

Hasta donde se tiene noticia, el Colegio de Abogados de Lima ha impartido algunos cursos de especialización al respecto. Además,

dada la importancia de sus funciones se exige la constante actualización del fedatario juramentado, bajo normas precisas de evaluación.¹³

En opinión de Carmen Velarde Koechlin, existen profundas diferencias entre este fedatario juramentado y el tradicional notario público:

El campo de actuación del Fedatario Juramentado se circunscribe a los actos realizados mediante el uso de equipos de nueva tecnología (por ello nuestra propuesta de titular al cargo como “Fedatario Juramentado en Informática”). Ello incluiría el otorgar certitud de los actos digitales y creaciones de documentos electrónicos. El Fedatario Juramentado no puede consignar escrituras públicas, ni actas de transferencias de bienes muebles registrables, etc. Redacta tan sólo cuatro tipos de actas: acta de apertura, acta de cierre, acta de retoma y acta de comprobación. Otorga testimonio de dichas actas y finalmente, autentica las copias impresas de las microformas.

El Fedatario Juramentado, entonces reviste menos funciones. La propia norma reconoce la mayor potestad notarial. Por ejemplo, se exige al Fedatario Juramentado el uso de libros de registro de actas. Culminadas sus funciones como tal, dichos libros y todo su legajo será trasladado al notario más cercano de su jurisdicción, tal como lo dispone el art. 19 del Reglamento: “En caso de que por cualquier razón deje de actuar un fedatario juramentado, sus archivos de actas serán entregados a una notaría del lugar, para su conservación y administración”. Agrega este artículo que el juez civil aprobará esta medida. El reglamento también dispone que el Fedatario juramentado puede laborar en una notaría, en cuyo caso se le calificará como funcionario público.

El Fedatario Juramentado, se convierte, entonces, en un apoyo al notariado, ya que los documentos a traspasa del papel hacia los soportes tecnológicos son abundantes. Los notarios públicos no abastecerían la demanda del mercado y su presencia constante en los procesos de un funcionario que sólo otorgue certeza de los procesos realizados mediante el uso de equipos de nueva tecnología —actuando en el

¹³ “Los Fedatarios Públicos y Particulares juramentados deberán periódicamente, una vez obtenido el certificado de idoneidad técnica, tener una capacitación continua a través de cursos, seminarios de actualización y especialización que serán organizados por el Colegio de Abogados y/o por el Colegio de Notarios de su jurisdicción, en concordancia con lo establecido en el art. 6º del D. S. N° 009-92-JUS. Esta obligación deberá ser cumplida en forma constante por los Fedatarios Públicos y Privados y generará el puntaje que precise el reglamento, para efectos de su ratificación cada cinco años. La ratificación será realizada por el Colegio de Abogados y/o Notarios que emitió el certificado de idoneidad técnica, previa evaluación académica, conforme el procedimiento precisado en el Reglamento.”

mercado, paralelamente al notario— permitirá una mayor eficacia en los procesos de micrograbación.¹⁴

7. UTAH DIGITAL SIGNATURE ACT, UTAH, 1995

Utah fue el primer estado en todo el mundo en regular de manera amplia el fenómeno del comercio electrónico y las firmas digitales. En efecto, dicho estado expidió su *Digital Signature Act* el 27 de febrero de 1995 y fue legalmente promulgada por Michael Leavitt, gobernador del estado. Entró en vigor el primero de mayo de 1995.

La Ley de Firmas Digitales en Utah abarca todo el Capítulo Tercero del Título 46 de la compilación legislativa local en el estado. Así, según el estilo legislativo anglosajón, la ley inicia en el Título 46, Capítulo Tercero, § 101 (46-3-101).

Consta de un total de cinco partes que se tratan del título, interpretación y definiciones de los términos más usuales (Primera Parte); al licenciamiento y regulación de las entidades certificadoras (Segunda Parte); a las obligaciones de estas entidades certificadoras y del suscriptor (Tercera Parte); a los efectos legales de la firma digital (Cuarta Parte) y al reconocimiento y confiabilidad de los licenciarios, así como a los servicios gubernamentales respectivos (Quinta Parte).

La ley define el término *firma digital* como la conversión de un mensaje utilizando una clave criptográfica que puede descifrarse con la llave pública del suscriptor y que, eventualmente, permite detectar su alteración.¹⁵

Se define también el vocablo *persona* como cualquier entidad, física o moral, capaz de suscribir un documento en tales condiciones.¹⁶

Esta ley de Utah no difiere substancialmente de la *Digital Signature Guidelines* y existe una gran similitud entre ambas. Por tanto,

¹⁴ Velarde Koechlin, Carmen, "El Fedatario Particular Juramentado en Informática: Institución peruana al servicio de una solución global": en *Revista Electrónica de Derecho Informático* (REDI), N° 08, marzo, 1999.

¹⁵ "Digital signature: means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether:

a) the transformation was created using the private key that corresponds to the signer's public key; and

b) the message has been altered since the transformation was made."

¹⁶ "Person: means a human being or any organization capable of signing a document, either legally or as a matter of fact."

sólo diré aquí que esta ley reitera atribuciones a la División, que es el organismo administrativo encargado de procesar los registros o archivos relativos a empresas. Su nombre oficial es *Division of Corporations and Commercial Code (Utah Department of Commerce)*. Por cierto que esta División comisiona a lo que se denomina como *escribanos*, en términos de lo dispuesto en el art. 9º del Código Comercial de Utah.

Sus funciones se encuentran especificadas en el § 104, en un total de ocho reglas, que también especifican sus objetivos. Por cierto que entre sus atribuciones se encuentra la de generar otras autoridades certificantes que, a su vez, realicen la labor de emitir certificados para el sector privado.

Para obtener una licencia de autoridad certificante, se necesita lo siguiente:

ART. 201.—Acreditación...

1. Debe ser suscriptor de un certificado publicado en un repositorio reconocido;
2. Debe emplear como personal operativo sólo a personas que no hubiesen sido condenadas en los últimos quince años por delitos de fraude, falso testimonio o engaño;
3. Debe emplear como personal operativo sólo a personas que hubiesen demostrado tener conocimientos y la capacidad de cumplir con los requisitos del presente capítulo;
4. Debe presentar en la División una suficiente garantía, a menos que la autoridad certificante sea el gobernador, algún organismo del gobierno estadual, la Fiscalía de Estado, el Consejo Judicial de Utah, una ciudad o una municipalidad, siempre y cuando los mencionados actuaran a través de funcionarios designados, autorizados por ley o reglamento, a ejercer las funciones de autoridad certificante; y este Estado o uno de los organismos mencionados sea el suscriptor de todos los certificados emitidos por dicha autoridad certificante;
5. Debe tener la posibilidad de usar un sistema confiable, incluso un método seguro para controlar el uso de su clave privada;
6. Debe presentar a la División prueba de poseer un suficiente capital de explotación que le permita realizar negocios en calidad de autoridad certificante;
7. Debe tener oficinas en este Estado o contar con un representante matriculado para la notificación de actos procesales en este Estado, y
8. Debe cumplir con todos los demás requisitos exigidos por la reglamentación de la División.

En cuanto al reconocimiento de otras licencias:

La División puede reconocer la acreditación o autorización de autoridades certificadoras que realicen otros organismos gubernamentales, siempre y cuando los requisitos para la acreditación sean substancialmente similares a los que rigen en este Estado. En tal caso:

1. La parte 4 del presente capítulo, relacionada con las presunciones y efectos legales, regirá para los certificados emitidos por autoridades certificadoras acreditadas por dicho organismo gubernamental de la misma manera que rige para las autoridades certificadoras de este Estado, y
2. Los límites de responsabilidad del artículo 309 se aplicarán a las autoridades certificadoras acreditadas o autorizadas por dicho organismo gubernamental del mismo modo que rigen para las de este Estado. (Art. 201.)

Por su parte, el Título Tercero se refiere a las obligaciones de las autoridades certificadoras y de los suscriptores, especialmente a las reglas para la emisión, suspensión y revocación de certificados. Así, los requisitos previos para la emisión de un certificado son:

1. La Autoridad Certificante ha recibido un requerimiento de emisión firmado por quien será el suscriptor; y
2. La Autoridad Certificante ha confirmado que:
 1. El eventual suscriptor es la persona cuyo nombre figurará en el certificado a emitirse;
 2. Si el eventual suscriptor actúa a través de uno o más representantes, que los haya autorizado debidamente a tener la custodia de su clave privada y a requerir la emisión de un certificado donde aparezca mencionada la correspondiente clave pública;
 3. [La] información que aparece en el certificado es fidedigna;
 4. El eventual suscriptor posee legalmente la clave privada correspondiente a la clave pública mencionada en el certificado;
 5. El eventual suscriptor posee una clave privada capaz de crear una firma digital, y
 6. La clave pública a mencionarse en el certificado pueda utilizarse para verificar una firma digital generada por la clave privada que tiene el eventual suscriptor.

Los requisitos exigidos en el presente apartado son irrenunciables para la autoridad certificante acreditada, el suscriptor o ambos, según sea el caso. (Art. 302.)

A continuación, una vez que el suscriptor acepta el certificado emitido, la autoridad certificante publica una copia firmada en el

archivo oficial. Por cierto que esta publicación no es rigurosa, porque las partes pueden estipular en sentido contrario. También puede suceder que el suscriptor no acepte el certificado, en cuyo caso tampoco deberá publicarse y aun puede cancelarse su publicación si ya se hubiese hecho.

Mucho más adelante, los arts. 303-308 se refieren a las garantías y obligaciones de la autoridad certificante, a las consecuencias legales de la aceptación del certificado, al control de la clave privada, a la suspensión, revocación y al vencimiento del certificado.

Por último, el Título Cinco se refiere a los archivos o, como dice la ley, repositorios. La función de estos archivos es solamente informar y, por lo tanto, no se asume ninguna responsabilidad por la información contenida en los certificados. Los requisitos para el reconocimiento oficial de los archivos son los siguientes:

La División reconocerá a uno o más repositorios, cuando haya constatado:

1. Que el repositorio a ser reconocido opera bajo la dirección de una autoridad certificante acreditada;
2. Que incluye una base de datos que a su vez contiene:
 1. Certificados publicados en el mismo;
 2. Notificaciones de certificados suspendidos o revocados, publicadas por las autoridades certificadoras acreditadas u otras personas que suspenden o revocan certificados;
 3. Registros de publicidad de autoridades certificadoras acreditadas;
 4. Todas las órdenes o recomendaciones publicadas por la División para regular a las autoridades certificadoras, y
 5. Toda otra información que determinen las normas de la División.
3. Que opera mediante un sistema confiable;
4. Que no contiene una cantidad significativa de información que la división considere que es, o puede ser, no fidedigna o insuficientemente confiable.
5. Que contiene certificados publicados por autoridades certificadoras a quienes se les requiere cumplir con las normas de uso que la División considera substancialmente similares, o más estrictas hacia las autoridades certificadoras, que las de este Estado;
6. Que lleva un archivo de los certificados que han sido suspendidos o revocados, que han expirado, por lo menos en el término de los últimos 3 años, y
7. Que cumple con todo otro requisito razonable prescrito por las normas de la División. (Art. 501.)

La solicitud debe hacerse precisamente en las oficinas de la División, con los anexos probatorios del caso. El permiso se concede en términos de lo dispuesto en la Ley de Procesos Administrativos (Título 63, Capítulo 46 b). De esta forma, la autoridad se cerciora de que se cumplan con los extremos contenidos en los arts. 502 que se refiere a la responsabilidad, en el 406 (1) que se refiere a la certeza de la emisión del certificado con firma digital y asimismo a la aceptación del suscriptor y, por último, en el art. 201 (1) que se refiere a los requisitos para obtener la licencia y que ya he descrito aquí.

El objetivo final, como ve, reside en la creación de una red abierta de archivos con una serie de depósitos en libre competencia, si bien funcionando con criterios uniformes, para de esta manera facilitar su operación al máximo nivel posible de economía y funcionalidad. De todas formas, es cierto que la ley es insistente en el sentido de que no resulta obligatorio el registro en el archivo (de igual manera, la autoridad certificante sí tiene la obligación de ser suscriptor de un certificado publicado en un archivo oficial [art. 201.1]). En este punto debe verse, además, que el Código Administrativo fija normas relacionadas con los archivos.

Por último, conviene añadir que en este estado de Utah se encuentra en vigor una ley que, desde 1998, autoriza el uso de firmas digitales en el campo específico de los *Notaries Public* (Utah SB 107 de 11 de marzo de 1998).

8. *DIGITAL SIGNATURE GUIDELINES (ABA), USA, 1996*

La *American Bar Association (ABA)* desempeñó un papel importante en el desarrollo de la primera ley original en Utah y en sus reformas, que tuvieron lugar un año después, en 1996. Esta *American Bar Association* presentó valiosas sugerencias a través de su *Information Security Committee (Section of Science and Technology)* y luego habría de redactar una especie de legislación modelo denominada *Digital Signature Guidelines* (conocida informalmente como “*ABA Guidelines*”) cuyo propósito era describir de manera genérica y comprehensiva ciertos principios legislativos que podrían servir de guía para la unificación de criterios acerca de las firmas digitales en los distintos sistemas jurídicos.¹⁷

¹⁷ “[A] General, abstract statements of principle, intended to serve as long-term, unifying foundations for digital signature law across varying legal settings... a common

La Guía condensa, así, una serie de principios generales con los cuales se busca influenciar legislaciones de orden positivo. He aquí algunos de los más importantes:¹⁸

1.9 *Firmas digitales*. La transformación de un mensaje usando un sistema criptográfico asimétrico de modo tal que una persona teniendo el mensaje inicial y la llave pública del signatario pueda determinar sin lugar a dudas:

- (1) si la transformación fue creada usando la llave privada que corresponde a la llave pública del signatario, y
- (2) Si el mensaje inicial ha sido alterado desde que la transformación fue realizada.

...

1.16 *Mensaje*. La representación digital de una información.

1.17 *Notario*. La persona física autorizada por la ley para llevar a cabo servicios notariales tales como recibir un reconocimiento, un juramento o declaración, un testimonio o el reconocimiento de una firma o efectuar el protesto de un instrumento negociable.

...

1.19 *Persona*. La persona física o moral capaz de suscribir un documento, ya sea legalmente o en la práctica.

...

1.23 *Destinatario*. La persona que recibe o posee una firma digital y la asume como propia.

framework of unifying principles that may serve as a common basis for more precise rules in various legal systems.”

¹⁸ Debe existir traducción oficial al español de la Guía, preparada por la Unión Internacional del Notariado Latino. No la tengo en mi poder. Transcribo el texto original de los párrafos relativos:

1.9 Digital signature. A transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine

(1) whether the transformation was created using the private key that corresponds to the signer's public key, and

(2) whether the initial message has been altered since the transformation was made.

1.16 Message. A digital representation of information.

1.17 Notary. A natural person authorized by law to perform notarial services such as taking an acknowledgment, administering an oath or affirmation, witnessing or attesting a signature, and noting a protest of a negotiable instrument.

1.19 Person. A human being or any organization capable of signing a document, either legally or as a matter of fact.

...

1.23 Recipient. A person who receives or has a digital signature and is in a position to rely on it.

1.24 Repository. A system for storing and retrieving certificates or other information relevant to digital signatures.

...

1.26 Signer. A person who creates a digital signature for a message.”

1.24 *Registro*. Un sistema para almacenar y recuperar certificados o cualquier otra información concerniente a firmas digitales.

...

1.26 *Suscriptor*. La persona que dispone de una firma digital para un mensaje.

La definición de *Autoridad Certificadora* se encuentra en el art. 1.6. En términos muy lacónicos, se dice que “Autoridad certificadora es la persona que expide un certificado”, sin consignar mayores datos. Sin embargo, en los comentarios de este texto se trata de los requisitos para convertirse en autoridades certificadoras. La ley dice en el comentario que el “aseguramiento de la calidad” es el principal punto que debe satisfacer. Sin embargo, otros puntos importantes residen, también, en la satisfacción de elementos tales como la competencia y la responsabilidad profesional.

Desde luego, la experiencia y la reputación en las prácticas de certificación es muy importante. De esta forma puede graduarse el nivel de responsabilidad atendiendo a los recursos tecnológicos empleados y al rango de certificación que cubra la empresa. Así, quienes exijan el máximo nivel de responsabilidad porque se trate, por ejemplo, de proteger transacciones de alto valor económico o riesgo importante, buscarán empresas que precisamente confieran el más alto nivel de responsabilidad por riesgos. Si esto es así, acudirán entonces a la empresa que, en virtud de la satisfacción de los requisitos más exigentes, haya alcanzado por tanto el nivel más alto de certificación.¹⁹

Interesa en este aspecto mencionar específicamente la figura de los *CyberNotaries*, quienes pueden ser autoridades certificadoras a

¹⁹ “§ 1.6 Certification authority.

A person who issues a certificate.

1.6.1. Quality assurance should be a principal concern in selecting and utilizing certification authorities. Governmental regulation, professional accreditation, trade usage, auditing, and liability for negligent errors and omissions are examples of approaches toward assuring quality in certification authority practice.

1.6.2. Subject to applicable law, any person who undertakes the functions of a certification authority under these Guidelines may become a certification authority. The level of authority and reliance to be accorded to the certificates of the certification authority will be determined in part by the experience and reputation of the certification authority, and in part from the material presented in the certification practice statement. Those who seek a low level of responsibility to protect transactions of minor value or limited risk may accept a certificate of lower level assurance from a certification authority of unknown reputation. Those who seek the highest level of responsibility to protect transactions of high value and severe risk will obtain certificates providing the highest level of assurance, from certification authorities whose experience has earned them the highest respect.”

través de abogados admitidos a la práctica del litigio en los Estados Unidos (comprende el Distrito de Columbia y Puerto Rico) y, además, están autorizados para actuar como tales bajo las reglas específicas de un comité especial (*CyberNotary Committee*). Este *Cybernotary Committee* depende de la propia *American Bar Association* a través de su sección de ciencia y tecnología.

La función principal del cibernotario se concentra principalmente en transacciones electrónicas internacionales, especialmente en aquellas del más alto nivel de certificación o bien, en la prestación de servicios específicos de seguridad informática. Por tanto, es obvio que el cibernotario debe encontrarse en el más alto nivel exigido para la expedición de certificaciones.

Además de todo ello, los notarios estadounidenses y particularmente el cibernotario, pueden llegar a proveer varios servicios colaterales, por ejemplo, autenticaciones notariales que certifiquen incluso no solamente la firma, sino la validez legal de la propia transacción.²⁰

Por su parte, el certificado (*Certification authority certificate*) se define en los siguientes términos: “Es el documento que registra una autoridad de certificación como suscriptora y contiene una

²⁰ Este es el texto íntegro de los artículos 1.6.3 y 1.6.4:

“1.6.3 A notary or CyberNotary may be a certification authority, and serving as a certification authority may well be a natural extension of such a persons professional expertise, discipline, and practical experience. CyberNotaries are attorneys at law admitted to practice in the United States and qualified to act as a CyberNotary pursuant to specialization rules currently under development in the CyberNotary Committee, Section of Science and Technology of the American Bar Association. A CyberNotaries function mirrors that of a notary, and is focused primarily on practice in international, computer-based transactions. Under the planned specialization rules, a CyberNotary would possess technical expertise to facilitate computer-based transactions requiring a high level of certification, authentication, or other information security services. It is proposed that a CyberNotary would be required to meet a level of qualification as a legal professional commensurate with that of a notary, be a member in good standing of the bar of a state or territory of the United States, the District of Columbia, or Puerto Rico, be a member of the American Bar Association, and demonstrate technical competence in computer-based business transactions. For further information, contact the CyberNotary Committee, Section of Science and Technology, of the American Bar Association.

1.6.4 Moreover, notaries and CyberNotaries provide important adjunct services in addition to assuring the validity of a signature; for example, a notarial authentication in certain legal systems assures the validity and legal efficacy of the transaction itself, not merely its signatures. Notaries and CyberNotaries, therefore, may be well suited to serving as certification authorities, subject, of course, to satisfaction of the standards of training and practice required of all certification authorities by Guideline 3.1 (A certification authority must utilize trustworthy systems in performing its services.) and Guideline 1.35 (the definition of computer hardware, software and procedures which meet the test of a trustworthy system).”

llave pública que se corresponde con una llave privada, usadas para firmar digitalmente otro certificado”.²¹

Ello está estrechamente relacionado con la Declaración de Prácticas de Certificación (*Certification practice statement*). Es interesante aclarar aquí que esta declaración puede comprender a su vez varios documentos, en una combinación de derecho público, contratos privados y declaraciones en general, según se comenta en el punto 1.8.1.

9. FLORIDA ELECTRONIC SIGNATURE ACT, 1996

En 1996 se expidió la Ley de Firmas Electrónicas en el estado de Florida (*Electronic Signature Act*). Interesa reseñarla aquí no solamente por su avanzada previsión, sino especialmente por el hecho de que en Florida se dictó la ley de notarios de derecho civil (*Civil-law notary*, 1998) que busca la equiparación de los notarios locales con los notarios de tipo romanizado o latino.²²

El § 282.71 de la Ley de Firmas Electrónicas de Florida consigna sus propósitos, que se reducen a la promoción del desarrollo económico, la eficiente prestación de servicios gubernamentales a través de mensajes electrónicos, el incremento de la confianza del público en el uso de firmas electrónicas y el deseo de atenuar la falsificación de las mismas.

En estos términos, la ley define la expresión *firma electrónica* (*electronic signature*) como cualquier tipo de letra, características o

²¹ “§ 1.7 Certification authority certificate.

A certificate which lists a certification authority as subscriber and contains a public key corresponding to a private key used to digitally sign another certificate.”

²² En efecto, un famoso reporte de 30 de noviembre de 1996 del Departamento de Estado de Florida (*Electronic Commerce in Florida. Report to the Joint Legislative Committee on Information Technology Resources*, Florida Department of State) recomendaba la creación de abogados-notarios que gozarían entonces de la confianza de sus congéneres latinos, agregando que ningún otro estado de la Unión Americana había promovido una especialización similar y que la creación de esta nueva figura jurídica podría significar la atracción de importantes recursos financieros internacionales al estado de Florida.

Así, el capítulo 117 (*Chapter 117*) se refiere a *Notaries Public* y el capítulo 118 se refiere a la figura del *Civil-law notary* (*Chapter 118.10*). Es sumamente interesante el § 117.20 que se refiere a *electronic notarization*, aun dentro de la ley de los *notaries public* que llamaremos “tradicionales”.

La figura del notario de *Civil-law* está definida como aquella persona que es miembro de pleno derecho de *The Florida Bar*, que ha practicado la abogacía por al menos cinco años y que ha sido designado por la Secretaría de Estado como tal (§ 118.10 [b]). Este notario de *Civil-law* está autorizado para autenticar ciertos actos, recibir juramentos, efectuar certificaciones e incluso para certificar la celebración de matrimonios. Sus facultades incluyen todas las de los *notaries public* “tradicionales”.

símbolos manifestados por medios electrónicos o similares, ejecutados o adoptados por una parte con el propósito de autenticar un escrito. Se considera que un escrito se encuentra electrónicamente suscrito si una firma electrónica debe asociarse, de manera lógica, con tal escrito.²³

El § 282.73 se refiere precisamente a las consecuencias de esta firma electrónica especificando que debe tener la misma fuerza legal que la firma escrita por medios convencionales.²⁴

La autoridad competente para expedir certificados con el propósito de verificar firmas digitales o para adoptar o modificar reglas sobre el tema, es la Secretaría de Estado.

La definición que esta ley de Florida contiene con respecto a las autoridades certificadoras es muy sencilla, porque se reduce a decir que la autoridad de certificación es la persona que expide un certificado.²⁵

Como en el caso de leyes similares estadounidenses, la sección 6 establece que la Secretaría de Estado tendrá autoridad para la expedición de certificados que tengan el propósito de verificación para firmas digitales y adoptará las medidas necesarias para la suspensión de estas leyes incluyendo la revocación de los certificados expedidos. Se establece también que la Secretaría de Estado de Florida impondrá las tasas necesarias por los servicios. Es importante mencionar que de conformidad con lo dispuesto en este mismo artículo *in fine* “nada en este artículo debe ser interpretado como la obligación de ninguna empresa pública o privada para participar en el programa de certificación de la Secretaría de Estado, ni a ostentarse como autorizada, en los términos de este mismo artículo, para la verificación de firmas digitales”.²⁶

²³ “Electronic signature: means any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing. A writing is electronically signed if an electronic signature is logically associated with such writing (282.72 [4]).”

²⁴ “282.73 Force and effect of electronic signature.- Unless otherwise provided by law, an electronic signature may be used to sign a writing and shall have the same force and effect as a written signature.”

²⁵ “Certification authority: means a person who issues a certificate.”

²⁶ “Nothing in this section shall be construed to compel any public or private entity to participate in the Secretary of State’s certification program, as authorized in this section, in order to verify digital signatures.”

10. ILLINOIS ELECTRONIC COMMERCE SECURITY ACT, ILLINOIS, 1999

La más reciente de todas estas leyes es la *Illinois Electronic Commerce Security Act*, que entró en vigor en julio de 1999. Se trata de una ley bastante extensa, dividida en cuatro partes. La Primera Parte se refiere a los registros y a las firmas electrónicas en general (§5). La Segunda Parte se refiere a la confiabilidad de los instrumentos electrónicos, precisando los requisitos que deben reunirse para asegurar la confianza del público en el uso de estos medios (§10). La Tercera Parte previene sobre el uso y consecuencias legales de la firma digital y especifica las formas en que este tipo de suscripción minimiza los riesgos en la contratación electrónica (§15). El §20 establece las obligaciones de los suscriptores para obtener, aceptar y revocar un certificado. Finalmente, la Cuarta Parte (§25) se refiere a las agencias gubernamentales que intervienen en el proceso.

La sección 5-105 de esta ley define los términos “autoridad de certificación” y “declaración de prácticas de certificación”, casi en los mismos términos que otras leyes similares.²⁷

En el estado de Illinois la autoridad responsable de la certificación de los procedimientos electrónicos de seguridad es la Secretaría de Estado, de conformidad con lo dispuesto en la sección 10-135, en el marco de las secciones 10-105 y 10-110, que se refieren a registros y firmas electrónicas confiables. Así, se establece expresamente en el art. 10-135 inciso e) que esta Secretaría tendrá autoridad exclusiva para la certificación de procedimientos de seguridad bajo esta ley. En uso de sus atribuciones, la Secretaría de Estado puede considerar la opinión de expertos independientes, tales como *American National Standards Institute* (ANSI), *International Standards Organization* (ISO), *International Telecommunications Union* (ITU) y *National Institute of Standards and Technology* (NIST).

Los artículos siguientes tratan, como es usual, de los procedimientos de expedición, suspensión y revocación de los certificados.

²⁷ “Article 5. Electronic records and signatures generally.

Certification authority: means a person who authorizes and causes the issuance of a certificate.

Certification practice statement: is a statement published by a certification authority that specifies the policies or practices that the certification authority employs in issuing, managing, suspending, and revoking certificates and providing access to them.”

11. *ELECTRONIC TRANSACTIONS ACT, ALABAMA*

En el caso de Alabama interesa destacar solamente el capítulo especial que dedica a los efectos legales de lo que se llama *notarization*, ya que en virtud de este término legal se denomina la práctica de elevación a escrituras públicas, reconocimientos, certificaciones y declaraciones bajo fe de las firmas electrónicas de personas autorizadas para ejecutar tales actos, siempre y cuando la firma pueda ser reputada como lógicamente asociada con la persona que la expide o la asume como propia.²⁸

Por otra parte, la sección 17 se refiere a la creación y conservación de registros electrónicos, así como a la conversión de registros escritos por agencias gubernamentales y aceptación y distribución de los mismos, involucrando todo el proceso de creación, generación, comunicación, almacenamiento, procesamiento y confianza en los registros y firmas electrónicas.

Por último, la sección 19 autoriza a las agencias gubernamentales para la adopción de estándares o modelos que puedan ser operables con otras agencias gubernamentales en el resto de la Unión Americana, así como con particulares.

12. *DIGITAL SIGNATURE, TEXAS, 2000*

Corresponde ahora examinar lo relativo a las firmas digitales de Texas. Esta ley tuvo cambios importantes el 31 de marzo de 2000. Aunque contiene términos muy similares al resto de sus congéneres, es importante destacar aquí la definición específica consignada en el § 201.14 (b). En efecto, en el número 10 se define la figura del *escrow agent* en la forma siguiente: “es la persona que guarda o custodia una copia de la llave privada a solicitud del dueño, de una manera confiable”.²⁹

Esta ley, además, se mantiene en el criterio de enumerar la lista de tecnologías aceptables bajo una serie de criterios establecidos en el Código de Gobierno (*Government Code*), § 2054.060. Entre ellas

²⁸ “Section 11. Notarization and acknowledgment.

If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.”

²⁹ “(10) Escrow agent: a person who holds a copy of a private key at the request of the owner of the private key in a trustworthy manner.”

se encuentran las denominadas *Public Key Cryptography* y *Signature Dynamics*. De todas formas, en esta misma ley se establecen otros criterios específicos de manera bastante detallada y asimismo se deja abierta la posibilidad para añadir nuevas tecnologías a la lista.

13. *ELECTRONIC RECORDS AND SIGNATURES ACT, MASSACHUSETTS, 1998*

En este caso cabe destacar que el proyecto consagra en una sección específica las funciones de la *Chief Information Officer*, quien tendrá la autoridad para coordinar, supervisar y aprobar el uso de tecnologías de seguridad y autenticación informática por cualquier ente público de la Oficina Ejecutiva de Administración y Finanzas.

Otra novedad importante consiste en la sección 108 que autoriza el uso de registros y firmas electrónicas por empresas (*Business Entities*): según este artículo, un contrato realizado entre estas empresas no podrá ser rechazado bajo el argumento simple de que aparezca como firmado con una firma electrónica.³⁰

14. *REGOLAMENTO RECANTE CRITERI E MODALITÀ PER LA FORMAZIONE, L'ARCHIVIAZIONE E LA TRASMISSIONE DI DOCUMENTI CON STRUMENTI INFORMATICI E TELEMATICI, LEGGE 15 MARZO 1997, N. 59*

Desde 1996, la República Italiana mantenía bajo estudio un interesante proyecto sobre documentos electrónicos que trataba los temas referentes a los requisitos del documento informático, su valor y eficacia probatoria, las claves asimétricas de codificación, la responsabilidad por el uso de las claves secretas, la firma digital, su oponibilidad a terceros, la contratación por medios electrónicos, las autoridades certificadoras y un registro único de claves criptográficas públicas.

Pues bien, el 15 de marzo de 1997 se expidió la ley número 59 que trata sobre el tema. A continuación hubo de dictarse el reglamento respectivo que trata de los criterios y de las modalidades para la formación, el archivo y la transmisión de documentos a través de medios informáticos y telemáticos, aparecido en la *Gazzetta Ufficiale* número 60 de 13 de marzo de 1998.

El reglamento es muy amplio. Contiene un total de veintidós artículos bastante prolijos. La estructura de la ley se encuentra

³⁰ "Section 108. Use of Electronic Records and Electronic Signatures by Business Entities.

conformada por sólo tres capítulos que se refieren a los principios generales, a las firmas digitales y a las normas de actuación. Así, el art. 1 del reglamento consigna las definiciones que ya son usuales en el tema, considerando por ejemplo que por *firma digital* debe entenderse el resultado de un cierto procedimiento de validación informática basado sobre un sistema de llaves asimétricas dobles, una pública y otra privada, que permite al suscriptor —a través de la llave privada— y al destinatario —a través de la llave pública— respectivamente, verificar el origen y la integridad de un documento informático o de un conjunto de documentos informáticos.³¹

Al tenor del art. 4º, se prescribe que el documento informático provisto de los requisitos exigidos en el presente reglamento satisface la exigencia legal de la forma escrita.³² Así, su eficacia probatoria se extiende a la de un documento privado en los términos de los arts. 2702, 2712 y 2214 del *codice civile*.³³

Por otra parte, el nuevo reglamento italiano de documentos informáticos y telemáticos de 1998 trata con detalle el tema y en su art. 16 consigna el caso de la autenticación de firmas electrónicas por notario, reconociendo que en el sentido previsto por el art. 2703 del *Codice*, la intervención de un notario o de otro oficial público autorizado, confiere plenos efectos legales a dicha firma.³⁴

(a) A contract between business entities shall not be unenforceable, nor inadmissible in evidence, on the sole ground that the contract is evidenced by an electronic record or that it has been signed with an electronic signature. For purposes of this section, "contract" shall mean a contract for the sale of goods or services, for the sale or license of digital information, or for the lease of tangible personal property. The provisions of this subsection shall not apply if their application would involve a construction of a rule of law that is clearly inconsistent with the purpose of that rule of law, provided that the mere requirement that information be "in writing", "written", "printed", or "signed", or use of any other word that purports to specify or require a particular communications medium, shall not by itself be sufficient to establish such purpose."

³¹ "1. Ai fini del presente regolamento s'intende: b) per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici."

³² "1. Il documento informatico munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta."

³³ Así, el art. 2702 dice: "La scrittura privata fa piena prova, fino a querrela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta." (*Codice Civile* italiano.)

³⁴ Es importante aclarar aquí, sin embargo, que los notarios italianos ya tenían contemplado en su *Ordinamento del Notariato e degli Archivi Notarili* (16 de febrero de 1913) y en el Reglamento respectivo (10 de septiembre de 1914) la posibilidad de transmitir

Para el caso es necesario que se reúnan los siguientes requisitos: que la firma digital haya sido puesta en presencia del titular; que éste haya verificado su identidad personal; que se haya constatado la validez de la llave utilizada, que el documento suscrito responda a la voluntad del suscriptor y que no contravenga disposición legal alguna (art. 16.2).

La certificación de esta firma digital por el fedatario público sustituye, para todo tipo de efectos legales, la imposición de sellos, punzones, timbres, contrasellos y marcas de cualesquier naturaleza (art. 16.3).

También se previene el caso de que a este documento informático, ya autenticado, deba ser agregado otro documento original, por ejemplo, en soporte papel. Si es así, el notario puede relacionar la copia informática autenticada siguiendo lo dispuesto en el diverso art. 6º de este mismo reglamento que se refiere a las copias de los actos y documentos, aun en distintos tipos de soporte documental (6.1).

La firma digital que aparezca en el documento informático que se presente o deposite en cualquier oficina pública se considera como verificada en presencia del funcionario correspondiente, en

actos pasados ante su fe por vía telegráfica o telefónica (arts. 71 y 85 respectivamente), mediante un sencillo procedimiento con intervención de los funcionarios de las oficinas expedidora y receptora, en el caso de la comunicación vía telegráfica. Este es el texto de los artículos correspondientes:

“Art. 71 (*Ordinamento*). Il notaro può trasmettere il sunto o il contenuto degli atti, per telegrafo o per telefono.

...
Il sunto come sopra redatto, deve essere trascritto sugli appositi moduli per telegrammi, dal notaro, che vi farà precedere l'indicazione in lettere del numero di repertorio dell'atto e vi apporrà la propria firma, munita dell'impronta del sigillo.

L'ufficio telegrafico mittente assicurerà quello ricevente che il telegramma è stato spedito realmente dal notaro.

...
Quando si tratti di trasmissione per telefono, essa deve essere fatta e ricevuta rispettivamente e personalmente da due notari, i quali dovranno far risultare la loro identità e l'oggetto della comunicazione agli uffici telefonici.

Il notaro ricevente tradurrà in iscritto la comunicazione avuta e ne curerà la collazione col notaro trasmittente.”

“Art. 85 (*Regolamento*). Il notaro che trasmette per telegrafo, ai sensi dell'art. 71 della legge, il sunto o il contenuto di un atto deve firmare il modulo del telegramma in presenza dell'impiegato telegrafico, dopo aver fatto constare la propria identità.

...
Il notaro che trasmette per telefono il sunto od il contenuto di un atto, e il notaro che lo riceve, dovranno rilasciare una dichiarazione datata e sottoscritta alla presenza dell'impiegato telefonico, munita altresì dell'impronta del proprio sigillo. Tale dichiarazione deve contenere l'indicazione: *per trasmissione*, o *ricezione di contenuto* o *ricezione di sunto di atto notarile*.”

términos de lo dispuesto en el párrafo quinto de este mismo art. 14, que además remite al art. 3º, párrafo 11 de la *Ley no. 127* de 15 de mayo de 1997.

Existe una ventaja más: el depósito o la presentación de un documento por vía telemática o sobre un soporte informático en una oficina cualesquiera de la administración pública, resulta válido para todos los efectos legales si se han seguido las normas prescritas en este reglamento.³⁵

En el art. 1.1 inciso g) esta ley aclara que:

1.1. Debe entenderse en el presente reglamento:

...

g) por certificación, el resultado de un procedimiento informático, aplicado a la clave pública de una pareja de claves asimétricas obtenido por sistemas de validación mediante el cual se garantiza la exclusividad y particularidad de la pareja, su pertenencia a un sujeto y su periodo de validez.³⁶

³⁵ He aquí el texto íntegro del art. 16 de este reglamento:

“1. Si ha per riconosciuta, ai sensi dell’articolo 2703 del codice civile, la firma digitale, cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato.

2. L’autenticazione della firma digitale consiste nell’attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l’ordinamento giuridico ai sensi dell’articolo 28, primo comma, numero 1, della legge 16 febbraio 1913, n. 89.

3. L’apposizione della firma digitale da parte del pubblico ufficiale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell’originale, secondo le disposizione dell’articolo 6 del presente regolamento.

5. Ai fini e per gli effetti dell’articolo 3, comma 11, della legge 15 maggio 1997, n. 127 si considera apposta in presenza del dipendente addetto la firma digitale inserita nel documento informatico presentato o depositato presso pubbliche amministrazioni.

La presentazione o il deposito di un documento per via telematica o su supporto informatico ad una pubblica amministrazione sono validi a tutti gli effetti di legge se vi sono apposte la firma digitale e la validazione temporale a norma del presente regolamento”.

³⁶ “1.1. Ai fini del presente regolamento s’intende:

...

g) Per certificazione, il risultato della procedura informatica, applicata alla chiave pubblica di una coppia di chiavi asimmetriche, rilevabile dai sistemi di validazione, mediante la quale si garantisce la unicità ed univocità della coppia, la sua appartenenza ad un soggetto ed il periodo di loro validità.”

Por su parte, el Reglamento define también en su art. 1º inciso *h)* el mismo concepto, pero agrega en su inciso *m)* que debe entenderse “por certificador, el sujeto público privado que efectúa una certificación, expide el certificado de la clave pública, lo publica junto con ella y actualiza los registros de los certificados suspendidos y revocados”.³⁷

Este mismo Reglamento previene en su art. 8º (se refiere a certificaciones) que:

... las actividades de certificación son efectuadas por certificadores incluidos sobre la base de una declaración anterior al inicio de su actividad, en un directorio público, consultable en vía telemática, confeccionado y actualizado bajo la responsabilidad de la Autoridad para la Informática en la administración pública, con los siguientes requisitos...:

- a) Estar conformados como sociedad por acciones y capital social no inferior al necesario al que se pide en las autorizaciones por actividad bancaria, si se trata de particulares.
- b) Posesión de parte de los representantes legales y de los administradores, de los requisitos de honorabilidad exigidos a los sujetos que desempeñan funciones de administración, dirección y control en la actividad bancaria.
- c) Confianza que, por competencia y experiencia, los responsables técnicos del certificador y el personal empleado en esta actividad, respeten las normas del presente reglamento y las reglas técnicas respectivas del art. 3º.
- d) Calidad de los procesos informáticos y de los productos correspondientes sobre la base de modelos reconocidos a nivel internacional.³⁸

³⁷ “Per certifikatore, il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest’ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati.”

³⁸ “Art. 8 Certificazione

3. Salvo quanto previsto dall’articolo 17, le attività di certificazione sono effettuate da certificatori inclusi sulla base di una dichiarazione anteriore all’inizio dell’attività, in apposito elenco pubblico, consultabile in via telematica, predisposto, tenuto e aggiornato a cura dell’Autorità per l’informatica nella pubblica amministrazione, e dotati dei seguenti requisiti, specificati nel decreto di cui all’articolo 3:

- a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell’autorizzazione all’attività bancaria, se soggetti privati;
- b) possesso da parte dei rappresentanti legali e dei soggetti preposti all’amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche;
- c) affidamento che, per competenza ed esperienza, i responsabili tecnici del certifikatore e il personale addetto all’attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all’articolo 3;
- d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.”

Por lo que hace a los documentos extranjeros, este art. 8.4 consigna la misma regla:

El procedimiento de certificación de que se trata en el párrafo 1 puede ser desarrollado también por un certificador autorizado expedida por otro estado miembro de la Unión Europea o del espacio económico europeo sobre la base de requisitos equivalentes.³⁹

Las obligaciones del certificador se encuentran establecidas en el art. 9.2 en la siguiente forma:

El certificador está obligado a:

- a) identificar con certeza a la persona que solicita la certificación;
- b) expedir y publicar el certificado con las características de que trata el art. 3º;
- c) Especificar, previa solicitud y con el consentimiento de los terceros interesados, la subsistencia de los poderes de certificación o de otros documentos relativos a la actividad profesional o de los cargos con que se ostentan;
- d) Satisfacer la reglas técnicas de dicho art. 3º;
- e) Informar a los solicitantes, en forma clara y completa, sobre los procedimientos de certificación y los requisitos técnicos necesarios para cumplirlos;
- f) Atenerse a las medidas mínimas de seguridad para el tratamiento de los datos personales, de conformidad con lo dispuesto por el art. 15, párrafo 2, de la Ley N^º 675 de 31 de diciembre de 1996;
- g) No convertirse en depositario de claves privadas;
- h) Proceder inmediatamente a la revocación o a la suspensión del certificado en caso de solicitud del particular o del tercero del cual derivan los poderes de este último, de pérdida de la posesión de la llave, disposiciones de la autoridad, conocimiento de causas limitativas de la capacidad del titular o presuntos abusos y falsificaciones;
- i) Publicar inmediatamente la revocación y la suspensión de las parejas de claves asimétricas;
- j) Comunicar inmediatamente a la Autoridad para la Informática de la administración pública y a los usuarios, con al menos seis meses de anticipación, la cesación de la actividad y la inoperancia de la documentación o su anulación.⁴⁰

³⁹ "La procedura di certificazione di cui al comma 1 può essere svolta anche da un certificatore operante sulla base di licenza o autorizzazione rilasciata da altro Stato membro dell'Unione Europea o dello Spazio economico europeo, sulla base di equivalenti requisiti."

⁴⁰ "Art. 9º—...

...

15. *TELEDIENSTEGESETZ (TDG), SIGNATURGESETZ (SiG),
ALEMANIA, 1997*

En Alemania se expidieron sendas leyes sobre firmas digitales (*Gesetz zur digitalen Signatur*) y sobre la utilización de servicios a distancia (*Gesetz über die Nutzung von Telediensten*), aparecidas en la Gaceta de Leyes Federales (*Bundesgesetzblatt*) y que entraron en vigor el primero de agosto de 1997.

En rigor, esta Ley de Firmas Digitales alemana fue decretada como formando parte de una distinta Ley de Servicios de Información y Comunicación (*Informations- und Kommunikationsdienstes-Gesetz, IuKDG*), en su art. 3º. Su contenido se refiere a un párrafo inicial relacionado con el propósito y alcance de la ley y otros párrafos de definiciones relacionadas, autoridades competentes, régimen de licencias, expedición de certificados, contenido de los mismos, protección de la información, vigilancia y ejecución de las obligaciones consecuentes y certificados expedidos por entidades extranjeras.

A su vez, la diversa Ley de Servicios a Distancia fue decretada también como formando parte (art. 1º) de la ya mencionada Ley de Servicios de Información y Comunicación. El propósito de la Ley de Servicios a Distancia consiste en el establecimiento de condi-

2. Il certificatore è tenuto a:

- a) identificare con certezza la persona che fa richiesta della certificazione;
- b) rilasciare e rendere pubblico il certificato avente le caratteristiche fissate con il decreto di cui all'articolo 3;
- c) specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a caniche rivestite;
- d) attenersi alle regole tecniche di cui all'articolo 3;
- e) informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
- f) attenersi alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675;
- g) non rendersi depositario di chiavi private;
- h) procedere tempestivamente alla revoca od alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni;
- i) dare immediata pubblicazione della revoca sospensione della copia di chiavi asimmetriche;
- j) dare immediata comunicazione all'Autorità per l'informatica nella pubblica amministrazione ed agli autenti, con un preavviso di almeno sei mesi, della cessazione dell'attività e della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento."

ciones económicas uniformes para la aplicación de los servicios de la comunicación e información electrónicas.

En el contexto de esta ley, el vocablo “teleservicios” incluye los servicios ofrecidos en el campo de la comunicación individual, la información o comunicación —genérica—, internet y otras redes electrónicas, telejuegos y la oferta de bienes y servicios con acceso interactivo y la posibilidad de órdenes directas.

La ley aclara en su § 4 que para los propósitos de esta misma ley, los servicios a distancia reseñados no estarán sujetos a licencia o registro alguno.

Por último, también debe mencionarse la Ley sobre Protección de la Información Personal usada en los servicios a distancia (*Tele-dienststedatenschutzgesetz, TDDSG*), que constituye a su vez el art. 2º de la ley reseñada.

Esta ley alemana contiene las siguientes definiciones:

ART. 2º—Definiciones:

...

2. Un certificador dentro del significado de esta ley, es una persona física o jurídica la cual da fe a la atribución de claves públicas de firma a personas físicas y mantiene una licencia para ese motivo según el artículo 4º.

3. Un certificado, dentro del significado de esta ley, es una certificación digital rotulada con una firma digital respecto a la atribución de una clave de firma pública a una persona física (certificado de clave de firma), o una certificación digital especial que se refiere inequívocamente a un certificado de clave de firma y contiene información adicional (certificado de atributos).⁴¹

La autoridad reconocida encuentra su fundamento en el art. 66 de la Ley de Telecomunicaciones alemana. De conformidad con lo dispuesto en el art. 5 el procedimiento es el siguiente:

ART. 5º—Emisión de certificados de claves de firmas y sellos de fecha y hora:

⁴¹ “§ 2 Definitions:

...

(2) For the purposes of this Act “certification authority” shall mean a natural or legal person who certifies the assignment of public signature keys to natural persons and to this end holds a license pursuant to § 4 of this Act.

(3) For the purposes of this Act “certificate” shall mean a digital certificate bearing a digital signature and pertaining to the assignment of a public signature key to a natural person (signature key certificate) or a separate digital certificate containing further information and clearly referring to a specific signature key certificate (attribute certificate).”

1. El certificador deberá identificar fehacientemente a las personas que soliciten certificados. Deberá confirmar la atribución de una clave pública de firma a una persona identificada mediante un certificado de claves de firma y mantendrá acceso a estos, así como a los certificados asociados (párrafo 2), en todo momento y para cualquier persona, a través de conexiones de telecomunicaciones accesibles públicamente de una manera verificable y con el consentimiento del dueño de la clave de firma, salvo pedido explícito de no publicación por parte del suscriptor.
2. Bajo pedido de un solicitante, el certificador registrará información concerniente al poder de representación de una tercera parte o sus licencias profesionales u otras, en el certificado de clave de firma o en un certificado de atributos, en tanto se demuestra fehacientemente el consentimiento de la tercera parte para que tal licenciamiento o poder de representación sean registradas en un certificado.
3. A pedido de un solicitante, el certificador deberá registrar un seudónimo en el certificado en el lugar del nombre del solicitante.
4. El certificador deberá tomar medidas para que la información de los certificados no puedan ser alterados o falsificados de manera no visible. Deberá tomar medidas de modo que se garantice la confidencialidad de la clave privada. No es confiable el almacenamiento de claves privadas por parte del certificador. (Nota: El contenido de este apartado es cuestionable. El certificador nunca debe tomar contacto con las claves privadas de los suscriptores. Además, existen divergencias entre las versiones en inglés y en alemán.)⁴²
5. El certificador deberá usar personal confiable para el ejercicio de las actividades de certificación y deberá usar componentes técnicos de acuerdo a lo expresado en el artículo 14 para hacer accesibles las claves y para la generación de certificados. Esto se aplica también a los componentes técnicos que hacen posible la verificación de los certificados según párrafo 1, sentencia 2.⁴³

⁴² Copio la "nota" tal como aparece en el texto.

⁴³ "§ 5. Issue of Certificates:

(1) The certification authority shall reliably establish the identity of persons applying for a certificate. It shall confirm the assignment of a public signature key to an identified person by a signature key certificate which, together with any attribute certificates, shall be kept available for verification and, with the consent of the owner of the signature key, for retrieval at all times and for everyone over publicly available telecommunications links.

(2) At an applicant's request the certification authority shall include in the signature key certificate or an attribute certificate information relating to his authority to represent a third party and to his professional admission to practice or other type of admission insofar as reliable proof is furnished of the consent by the third party to the inclusion of the authority of representation or of the admission.

(3) At an applicant's request the certification authority shall indicate a pseudonym instead of the applicant's name in the certificate.

A su vez, el contenido de los certificados se encuentra especificado en el art. 7º:

ART. 7º.—Contenido de los certificados.

(1) Un certificado de clave de firma deberá contener al menos lo siguiente:

1. El nombre del dueño de la clave de firma, el cual se marca con una notación adicional si existe la posibilidad de confusión, o con un seudónimo inequívoco atribuible al dueño de la clave, el cual deberá ser identificado como tal;
2. La clave pública de firma atribuida;
3. El nombre de los algoritmos que pueden usarse con la clave pública del usuario, así como con la clave pública del certificador;
4. El número de serie del certificado;
5. El comienzo y el fin de la validez del certificado;
6. El nombre del certificador, y
7. Información acerca de la limitación de uso de la clave de firma a determinados tipos y ámbitos de aplicación.

(2) Información relacionada a la capacidad para representar una tercera parte y a la admisión profesional para practicar, o cualquier otro tipo de admisión, puede ser incluida tanto en el certificado de la llave de la firma como en el certificado de atribuciones.

(3) No debe ser incluida más información en este certificado a menos que las partes involucradas presten su consentimiento.⁴⁴

(4) The certification authority shall take measures to prevent undetected forgery or manipulation of the data intended for certificates. It shall also take measures to ensure confidentiality of private signature keys. Storage of private signature keys by the certification authority shall not be permitted.

(5) The certification authority shall engage reliable staff for the exercise of certification activities. For the provision of signature keys and the issue of certificates it shall use technical components as set out in § 14. This shall also apply to technical components enabling verification of certificates according to § 5 (1) sentence 2 above.”

⁴⁴ “§ 7 Content of Certificates.

(1) The signature key certificate shall contain the following information:

1. Name of the owner of the signature key to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the owner of the signature key, clearly marked as such;
2. Public signature key assigned;
3. Names of the algorithms with which the public key of the owner of the signature key and the public key of the certification authority can be used;
4. Serial number of the certificate;
5. Beginning and end of the validity period of the certificate;
6. Name of the certification authority, and
7. An indication as to whether use of the signature key is restricted in type or scope to specific applications.

(2) Information relating to the authority to represent a third party and to the professional admission to practice or other type of admission may be included both in the signature key certificate and in an attribute certificate.

(Nota: Debería incluir la fecha de emisión del certificado.)⁴⁵

Es importante mencionar aquí lo dispuesto en el art. 15 de esta Ley de Firmas Digitales alemana que se refiere a los certificados extranjeros, cuyo contenido es muy similar al de otras leyes que he analizado aquí:

ART. 15. Certificados extranjeros.

(1) Las firmas digitales que se puedan verificar con una clave pública de firma para la cual exista un certificado extranjero de otro estado miembro de la Unión Europea o de otro estado firmante del Tratado en el área económica europea son equivalentes a firmas digitales según esta ley, en tanto puedan demostrar un nivel de seguridad equivalente.

(2) El párrafo 1 también se aplica a otros estados en la medida en que se suscriban acuerdos internacionales relativos al reconocimiento de certificados.⁴⁶

16. *DIGITAL SIGNATURE ACT, HONG KONG, 2000*

En el caso de Hong Kong, interesa solamente destacar que esta Ley (*Digital Signature Act*), excluye de sus previsiones aquellos negocios que, a causa de su forma solemne o especial, no puedan realizarse sobre este soporte. Un ejemplo especial se refiere a los documentos utilizados en el proceso electoral. Además, también suelen encontrarse en esta categoría de actos excluidos todas aquellas disposiciones legales concernientes a documentos específicos de autoridades gubernamentales, así como documentos de trabajo y planes de desarrollo gubernamentales. Es interesante consignar que también se encuentran excluidos cierto tipo de documentos utilizados por tripulaciones aéreas para propósitos de navegación. Por último, lo están los documentos relacionados con el cumplimiento de obligaciones gubernamentales en franquicias internacionales.⁴⁷

(3) Further information shall not be included in the signature key certificate unless the parties concerned give their consent."

⁴⁵ Copio la "nota" tal como aparece en el texto.

⁴⁶ "§ 15 Certificates Issued by Other Countries.

(1) Digital signatures capable of being verified by a public signature key certified in another Member State of the European Union or in another State party to the Agreement on the European Economic.

Area shall be deemed equivalent to digital signatures under this Act insofar as they show the same level of security.

(2) Paragraph (1) above shall also apply to other states insofar as relevant supranational or intergovernmental agreements have been concluded."

⁴⁷ "These statutory provisions are excluded:

17. *ELECTRONIC COMMERCE PROMOTION COUNCIL OF JAPAN, 1998*

En Japón resulta particularmente importante analizar la solución específica que se ha dado al problema de las autoridades certificadoras con base en lo que se ha denominado *notario electrónico* (*electronic notary*). Esta figura se define como el procedimiento para garantizar la seguridad y la confianza del intercambio comercial electrónico que viaja en la red.⁴⁸ Algunas de sus funciones son las siguientes: transacciones comerciales electrónicas de empresa a empresa y de empresa a consumidor, operaciones domésticas, notificaciones y solicitudes de carácter electrónico, administración y representación, almacenaje, etc.

Todo ello funciona a través de un centro específico (*Electronic Notary Center*) que se encuentra ubicado en lugares cómodos para el usuario y que provén toda la gama de servicios que se espera encontrar.

El principio jurídico que sustenta toda esta actividad certificadora es el de libertad contractual, de modo que todos los contratos son concluidos bajo esta base doctrinal. Las actividades desarrolladas por estos Centros Notariales Electrónicos comprende las siguientes actividades:

“Modelo Uno”: Se caracteriza por la ausencia de cualquier mecanismo electrónico para la seguridad o confiabilidad en el intercambio electrónico. En todo caso, la única seguridad proviene de reglas humanas convencionales pactadas por anticipado. Un ejemplo de ello es el uso del correo electrónico sin ningún mecanismo de seguridad, pero donde ambas partes acuerdan el hecho

1. Due to the solemnity of the matter or document involved, i.e. provisions concerning the electoral process;

2. On operational grounds, e.g. provisions concerning the production of documents to Government authorities on the spot;

3. Due to the involvement of voluminous submissions and complex plans which would be difficult to handle electronically, e.g. provisions concerning submission of documents and plans to the works departments;

4. Because of international practices, e.g. provisions concerning documents to be kept by the flight crew for air navigation purposes; and

5. To ensure that Government would be able to meet its contractual obligations, e.g. provisions on the submission of trade-related documents which concern the franchise of the Tradelink.”

Esta interesante disposición debe relacionarse con lo dispuesto en el § 4º del ETA (Singapur) y el art. 4º —también— del Proyecto de Ley sobre Documentos Electrónicos (Chile), acerca de los negocios jurídicos que pueden ser objeto de este tipo de leyes.

⁴⁸ “A procedure to ensure the safety and reliability of electronic interchange commerce, etc., conducted over networks.”

de que si alguien recibe un correo, debe entonces dar acuse de recibo.

“Modelo Dos”: En este caso, pueden utilizarse en efecto algunos mecanismos de control y de seguridad electrónicos, pero que solamente en forma parcial reemplazan las previsiones convencionales. Así, los usuarios no poseen un mecanismo especial de control electrónico y, por tanto, las reglas correspondientes deben ser establecidas. Un ejemplo de ello consiste en usar una tarjeta de identidad personal; su cocontratante puede utilizar, a su vez, una tarjeta computarizada para almacenar alguna clave cifrada.

“Modelo Tres”: Este modelo se caracteriza por el hecho de que ambos usuarios disponen de mecanismos electrónicos idénticos, por ejemplo, algún protocolo estándar de seguridad en el sistema de correo electrónico.

“Modelo Cuatro”: Este modelo supone la adopción de un mecanismo electrónico de seguridad proporcionado por un tercero, el cual dispone de una estructura operativa, ya de carácter público o ya de carácter privado. Es el caso de la oficina notarial electrónica.

“Modelo Cinco”: El último modelo constituye una etapa ideal en el desarrollo de la seguridad electrónica. En este caso, cualquier regla humana convencional se ve reemplazada por mecanismos de seguridad electrónicos. Así, la información relacionada con el intercambio electrónico no requiere de ninguna intervención personal, excepto en el caso de las reglas previamente establecidas por el orden legal. Esta etapa no puede aún ser realizada.

Este sistema notarial electrónico también puede adaptarse en la estructura interna de varias empresas y no solamente a un nivel externo en relación con el consumidor. De todas formas, los servicios ofrecidos por los centros son tan amplios que pueden comprender, incluso, servicios tales como el arbitraje, a través de la recepción de registros negociales o pruebas al respecto, de modo que puedan depositarse en dicho Centro las evidencias que sustenten los alegatos de las partes en conflicto. En estos casos el Centro Notarial Electrónico puede actuar constatando la alta confiabilidad de la tecnología usada, enviando funcionarios al lugar del conflicto para certificar la validez legal o eficacia de las pruebas, expidiendo certificados que constaten situaciones en particular y hasta ofreciendo una garantía a tercero de la efectividad de las pruebas.

El servicio también puede comprender la certificación con respecto a la presentación oportuna, en fecha y hora, de toda clase de documentos o registros electrónicos como por ejemplo, registros de patentes, presentación de documentos, plazos legales de espera, fechas de conclusión de contratos, etc. También se puede certificar el contenido de una información, así como la personalidad de quien la expide, de quien la recibe y la fecha exacta de ambas circunstancias. Se comprende en este caso la guarda y custodia de la información.

Como es obvio, todos estos importantes servicios deben reunir los siguientes requisitos:

1. Autenticidad;
2. Legibilidad, y
3. Preservación de la información.

La estructura organizacional de estos Centros Notariales Electrónicos puede clasificarse en dos grandes categorías: instituciones públicas e instituciones privadas. Además, ya se ha dicho que puede también funcionar un servicio a nivel doméstico, es decir, al interior de una empresa.

Es importante aclarar aquí que toda esta información electrónica funciona bajo dos principios elementales, uno de carácter económico y otro de carácter jurídico. El principio económico reside en el libre mercado; el principio jurídico, a su vez, reside en la autoresponsabilidad del proveedor. Los requisitos más importantes exigidos a los proveedores de este tipo de servicios son la confiabilidad, la adopción de controles de seguridad, altos requerimientos tecnológicos, amplias facilidades al usuario, precios razonables y funcionalidad operativa.

Se espera que la notarización electrónica japonesa rinda grandes dividendos a mediano plazo. Hay una gran posibilidad de expansión económica no solamente en los proveedores típicos de los servicios notariales de certificación, sino también en tiendas de consumo, compañías de seguros, asociaciones comerciales, proveedores de servicios electrónicos, grandes centros comerciales, etc.

18. LEY DE FIRMAS DIGITALES, PUERTO RICO, 1998

La Ley de firmas Digitales de Puerto Rico se dictó el 7 de agosto de 1998 bajo el número 188. En ella se dan las siguientes definiciones (art. 3º):

...

(2) “Autoridad certificadora” es una persona que emite un certificado.

(3) “Autoridad certificadora licenciada” es una autoridad certificadora que posee una licencia en vigor expedida por el Departamento de Estado.

...

(6) “Certificado” es un documento electrónico el cual:

(a) identifica la autoridad certificadora que lo emite;

(b) nombra o identifica al subscriptor;

(c) consigna la clave pública del subscriptor; y

(d) está firmado digitalmente por la autoridad certificadora que lo emite.

Se dedica un capítulo especial al licenciamiento y reglamentación de las Autoridades Certificadoras Licenciadas, bajo los siguientes requisitos:

ART. 5º—Concesión de Licencias; Requisitos:

(1) Para obtener o retener una licencia, una autoridad certificadora deberá cumplir con los siguientes requisitos:

(a) ser el subscriptor de un certificado publicado en un banco de información reconocido;

(b) no emplear como personal de operaciones a personas que han sido convictas por delito grave o un delito que envuelva fraude, declaraciones falsas o engaño;

(c) emplear como personal de operaciones a personas que posean conocimientos y destrezas para cumplir con los requisitos establecidos en esta Ley;

(d) registrar en el Departamento una garantía suficiente, excepto, cuando la autoridad certificadora sea el Gobernador, un departamento o agencia del Gobierno, sus dependientes o municipios, la Rama Legislativa y la Judicial, siempre que cumplan con los siguientes requisitos:

(i) actúen a través de un funcionario debidamente autorizado por Ley, ordenanza o reglamento, para desempeñar y ejecutar las funciones como autoridad certificadora; y

(ii) que la entidad gubernamental sea suscriptor de todos los certificados emitidos por la autoridad certificadora;

(e) tener el derecho a usar un sistema confiable, incluyendo un método seguro para controlar el uso de la clave privada;

(f) presentar prueba al Departamento de que posee capital de trabajo suficiente, según las normas que aprueba el Departamento, que le permite hacer negocio como autoridad certificadora;

- (g) mantener una oficina en Puerto Rico o tener un agente designado para recibir emplazamientos en Puerto Rico; y
- (h) cumplir con todos los demás requisitos establecidos mediante reglamento por el Departamento.

El procedimiento para la expedición de licencias a las autoridades certificadoras es relativamente sencillo. Se causan derechos por la inscripción legal. Quien expide las licencias es el Departamento de Estado del Gobierno de Puerto Rico, quien será a su vez autoridad certificadora y podrá emitir, suspender y revocar certificados, según las circunstancias específicas (número máximo de certificados emitidos y límites acumulativos de responsabilidad según la autoridad certificadora o la empresa u organización).

Desde luego, este Departamento tiene también facultades para revocación y suspensión de licencias. Por otra parte, estas facultades se extienden al reconocimiento de otras licencias o autorizaciones si se satisfacen requisitos similares a los previstos en esta ley. El alcance legal de este equiparación comprende incluso todas las consecuencias legales aplicables a las demás autoridades certificadoras licenciadas en la isla.

Sea como fuere, resulta claro establecer que la efectividad o validez de una firma digital continúa inalterable, en términos de lo dispuesto en la última parte del art. 5º, salvo que se prevenga otra cosa por disposición expresa de las partes.

El art. 7 previene expresamente la investigación de las actividades de las Autoridades Certificadoras Licenciadas, consignando sanciones que van desde la suspensión o revocación de la licencia a la imposición de multa administrativa (que no excederá de \$5 mil USD por cada violación).

En términos del art. 9, los deberes de las autoridades son los siguientes:

Una autoridad certificadora licenciada o un subscriptor tiene la obligación de utilizar sistemas confiables para emitir, suspender o revocar los certificados, para publicar y notificar la emisión, suspensión o revocación de los certificados, y para producir la clave privada. La autoridad certificadora licenciada debe divulgar las prácticas de certificación y cualquier dato pertinente relativo a la confiabilidad de un certificado o de su capacidad para prestar los servicios. Como requisito previo a la divulgación de lo dispuesto en este artículo, la autoridad certificadora contratará los servicios de una persona particular para que realice una investigación y presente un informe por escrito.

A su vez, los requisitos de emisión del certificado son los siguientes:

ART. 10.—Emisión del Certificado.

- (1) el suscriptor presenta la correspondiente solicitud; y
- (2) la autoridad certificadora verifica lo siguiente:
 - (a) que el suscriptor es la persona a cuyo nombre se emitirá el certificado;
 - (b) que actúa mediante un agente que le autorizó a tener bajo su custodia la clave privada y a requerir la emisión del certificado en que se designa la clave pública correspondiente;
 - (c) que la información contenida en el certificado a ser emitido es exacta;
 - (d) que el suscriptor es el tenedor legal de la clave privada que corresponde a la clave pública que se designa en el certificado;
 - (e) que el suscriptor es tenedor de una clave privada capaz de producir una firma digital, y
 - (f) que la clave pública indicada en el certificado puede ser utilizada para verificar una firma digital con la clave privada que tiene el suscriptor.

Las consecuencias legales de la emisión de este certificado comprenden las garantías y obligaciones de la propia Autoridad Certificadora, ya que el usuario debe confiar perfectamente en los siguientes extremos:

- (1) que la información contenida en el certificado es exacta;
- (2) que consideró toda la información pertinente y que los términos del certificado se basan en la misma;
- (3) que el suscriptor ha aceptado el certificado, y
- (4) que la autoridad certificadora licenciada ha cumplido con las leyes que reglamentan la emisión de certificados. (Art. 11.)

Enseguida, la Ley de Firmas Digitales consigna disposiciones para la suspensión, revocación y expiración del certificado en sus arts. 14-16.

También es importante advertir que las actividades de estas Autoridades Certificadoras Licenciadas serán auditadas por personal especializado por lo menos una vez al año. Esta información se transmite al registro de autoridades certificadoras.

Por último, en los términos de lo dispuesto en el art. 16, el certificado expira en la fecha que se encuentre precisamente prevista. Una vez llegado el término, debe entenderse que cesan com-

pletamente las obligaciones del suscriptor y de la Autoridad Certificadora. Como es obvio, esto supone al mismo tiempo que la propia autoridad certificadora se libera de todas las obligaciones resultantes de la certificación de dicho documento.

Expiración del Certificado.

El certificado indicará la fecha de su expiración. Transcurrido dicho término cesarán las obligaciones del suscriptor y la autoridad certificadora cesará de certificar la información contenida en el certificado, según se dispone en esta Ley y queda liberada de las obligaciones que conlleva la emisión del certificado. (Art. 16.)

19. LEY MODELO SOBRE COMERCIO ELECTRÓNICO (UNCITRAL), 1996

En 1996 la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI, por sus siglas en español; UNCITRAL, por sus siglas en inglés) aprobó en su resolución 51/162 la Ley Modelo sobre Comercio Electrónico (en adelante, LMCE) publicada originalmente en árabe, chino, español, francés, inglés y ruso.

Esta ley forma parte de un conjunto de novedosas legislaciones de derecho uniforme patrocinadas por ciertos organismos internacionales preocupados por la codificación y uniformidad del derecho privado a nivel mundial. Otras legislaciones similares, por ejemplo, son la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (CISG, por sus siglas en inglés, Viena, 1980) y los Principios sobre los Contratos Comerciales Internacionales de UNIDROIT (PCCI, Roma, 1994).

La LMCE consta de un total de diecisiete artículos redactados en el estilo legislativo anglosajón; se encuentran estructurados en un total de cuatro capítulos divididos en dos grandes partes que se refieren al comercio electrónico en general y al comercio electrónico en materias específicas. La metodología de cada uno de los preceptos sigue una división articulada en párrafos identificados con números arábigos que a su vez se dividen en incisos alfabéticos e incluso, de ser necesario, en romanos en minúscula.

La ley contiene un capítulo preliminar de definiciones. En su parte general, define la expresión "información en forma de mensaje de datos" como "la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o simi-

lares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax". Define los vocablos "intercambio electrónico de datos" como "la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto" (art. 2).

Así concebido, el mensaje electrónico tendrá toda clase de efectos jurídicos. Esta disposición debe relacionarse con lo dispuesto en el art. 9 que prevé, a su vez, que esta "fuerza probatoria" debe hacerse consistir en la fidelidad de generación, archivo o comunicación del mensaje, en su integridad y en la identificación auténtica del iniciador, así como en "cualquier otro factor pertinente".

Tres cuestiones importantes se tratan inmediatamente después: una es la relativa a la *forma* de la información, donde el art. 6º reputa como satisfecho el requisito si la información que contiene el mensaje informático "es accesible para su ulterior consulta". No obstante ello y atendiendo a su condición de ley modelo, la sección tres de este mismo art. 6 deja abierta la redacción para los países que deseen aplicar excepciones al caso.

La segunda cuestión importante se refiere, como es natural, a la imposición de la *firma* en este mensaje. Al respecto, la LMCE prevé la utilización de un método de identificación de la persona y de aprobación de la información, siempre que resulte tan fiable como sea apropiado "a la luz de todas las circunstancias del caso" (art. 7º).

La tercera cuestión atañe, por último, al establecimiento y conservación del *original* siempre que se respete la integridad de la información y pueda ser presentada en forma consecvente (art. 8º).

Un punto esencial en la contratación electrónica reside precisamente en la formación del contrato a través del mensaje informático. Si de suyo ha presentado problemas la simple contratación entre personas no presentes, la formación —ahora— de este complejo proceso consensual informático alcanza derivaciones imprevistas. Es cierto, desde luego, que la oferta y su eventual aceptación pueden ser expresadas a través de medios informáticos y que, desde luego, no conviene negar la producción de efectos jurídicos a este tipo de convenciones por la única razón de utilizar este medio. Desde el punto de vista jurídico, sin embargo, la contratación entre no presentes por medios electrónicos debe asimilarse como ya se ha visto, a la negociación entre presentes. La sección 2 del

art. 11 mantiene la redacción abierta para el establecimiento de excepciones.

El mensaje adquiere relevancia a través de un *iniciador*, que es la persona que actúa en forma directa o en representación de otra enviando o generando el mensaje electrónico. Esta persona puede enviar el mensaje por sí, por alguna otra facultada para hacerlo o incluso por un programa que opere en forma automática.

En el otro extremo del proceso se encuentra el *destinatario* y por tal debe entenderse a la persona designada por el iniciador para recibir el mensaje en forma directa. Este destinatario puede comprobar la procedencia del mensaje aplicando el código previamente establecido por el iniciador.

Puede también acusar recibo, si tal cosa hubo de acordarse con el iniciador. En este caso, se requiere dicho acuse para considerar que el mensaje de datos fue enviado. Una vez recibido el acuse, la LMCE presume que el destinatario ha recibido el mensaje, aunque no prejuzga sobre la fidelidad de la correspondencia.

¿*Quid iuris* en el caso de que no se haya establecido la dación del recibo en alguna forma específicamente determinada? En esta hipótesis, la sección 2 del art. 14 dispone que se podrá efectuar el acuse mediante cualquier tipo de comunicación del destinatario o incluso un acto genérico que debiera bastar para indicar al iniciador del proceso que el mensaje, en efecto, se ha recibido. Si no es así, es decir, si no se ha establecido previamente ninguna conducta adecuada en el caso, el iniciador puede dar aviso al destinatario de la ausencia del acuse de recibo, fijando un plazo razonable para su recepción, terminado el cual podrá dar nuevo aviso al destinatario considerando que el mensaje no ha sido enviado.

Lo que sucede a continuación depende en gran medida de los sistemas informáticos en recepción. El art. 15 consigna que el mensaje “se tendrá por expedido cuando entre en un sistema de información” distinto al controlado por el iniciador o su intermediario. Así, el momento preciso de recepción del mensaje informático tiene lugar al acceder este último al sistema de información de destino.

Puede suceder, no obstante, que en el caso de personas morales o grandes empresas exista pluralidad de establecimientos tanto para el envío como para la recepción, y en este caso debe entenderse como involucrado en el proceso a aquel establecimiento que guarde la relación más estrecha con la operación respectiva; si no la hay, la imputación debe hacerse al establecimiento principal. El caso contrario consiste en la ausencia de establecimiento, ya del

iniciador o ya del destinatario, en cuya hipótesis se aplica la regla de recurrir al lugar de su residencia habitual.

La segunda parte de la LMCE se refiere al comercio electrónico en materias específicas relacionadas con el transporte de mercancías y los documentos relacionados. Al efecto, el art. 16 realiza una enumeración no exhaustiva de los actos que guarden relación con el contrato de transporte o con sus efectos.

La documentación relativa al transporte tiene relación con lo dispuesto en el anterior art. 6 que consigna la forma del mensaje estableciendo como regla genérica que la sustitución de mensajes informáticos por documentos no puede afectar la posición jurídica de los contratantes.

Ninguno de los artículos, como se ve, se refiere al establecimiento de autoridades certificadoras, ni a los requisitos que deben contener los certificados expedidos, ni al eventual establecimiento de un registro de datos.

20. PROYECTO DE RÉGIMEN UNIFORME PARA LAS FIRMAS ELECTRÓNICAS (UNCITRAL), 1996

En el marco de esta misma ley modelo de la CNUDMI sobre comercio electrónico se discute la expedición de un régimen uniforme para las firmas electrónicas. En efecto, en el informe del Grupo de Trabajo correspondiente a julio de 2000 se divulgó el examen detallado de cada uno de los artículos de este *Proyecto de Régimen Uniforme para las Firmas Electrónicas* (en lo sucesivo, *Proyecto*).

A través de un grupo específico de trabajo sobre comercio electrónico la CNUDMI ha desarrollado, con la colaboración de un grupo de expertos, algunos invitados y otros designados por los gobiernos y organizaciones internacionales interesados en el tema, un informe sobre las cuestiones jurídicas que plantea el problema de las firmas electrónicas y las entidades certificadoras.

Tal proyecto involucra temas correspondientes a las firmas numéricas, firmas electrónicas, entidades certificadoras, reconocimientos de firmas electrónicas extranjeras y otras cuestiones jurídicas relacionadas.

Los últimos documentos de que dispongo son de julio y septiembre de 2000. Se tratan los temas correspondientes a las definiciones necesarias en el tema de firmas electrónicas, sus requisitos, cualidades de la información original, determinación de la firma electrónica refrendada, autonomía de la gestión contractual cele-

brada, obligaciones del titular de la firma, confiabilidad y, por último, obligaciones de la entidad certificadora.

El *Proyecto* ha sido objeto de múltiples reuniones de trabajo, fundamentalmente en Viena y Nueva York, a través de sucesivas reelaboraciones de cada uno de los artículos en examen. El Grupo de Trabajo está integrado por todos los estados miembros de la Comisión, que ascienden a un total de treinta y ocho, incluido México. El informe final debe presentarse hasta mayo de 2001 en Viena.

Por lo pronto el *Proyecto* consta de un total de doce artículos y el texto sometido a la discusión final es el siguiente:

ART. 1º—

El presente Régimen será aplicable a todo supuesto en el que se utilicen firmas electrónicas en el contexto de actividades comerciales. No derogará ninguna norma jurídica destinada a la protección del consumidor.

La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación del presente Régimen:

El presente Régimen será aplicable a todo supuesto en el que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [...].

Respecto al art. 2 este proyecto dice lo siguiente:

Tras examinar el proyecto de artículo 1º, el Grupo de Trabajo decidió aplazar el examen de las definiciones que figuraban en el proyecto de artículo 2 hasta completar su examen de las disposiciones sustantivas del Régimen Uniforme.

ART. 3º—

Ninguna de las disposiciones del presente Régimen se aplicará de modo que excluya, restrinja o prive de efecto jurídico cualquier método [de firma electrónica].

ART. 4º—

1) En la interpretación del presente Régimen Uniforme habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.
2) Las cuestiones relativas a materias que se rijan por el presente Régimen Uniforme y que no estén expresamente resueltas en él serán dirimidas de conformidad con los principios generales en que se inspira el Régimen Uniforme.

ART. 5º—

Salvo que el presente Régimen o el derecho del Estado promulgante disponga otra cosa, las partes podrán convenir en apartarse del presente Régimen o en modificarlo [modificar su efecto].

ART. 6º—

1) Cuando la ley requiere la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos si se utiliza [un método] [una firma electrónica] que es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

2) El párrafo 1) será aplicable tanto si el requisito previsto en él está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

ART. 7º—

1) Se presumirá que un mensaje de datos está en su forma original cuando, en relación con ese mensaje de datos, se utilice [un método] [una firma electrónica] [de acuerdo con el artículo 6º] que:

a) Ofrece alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma; y

b) De requerirse que la información sea presentada, dicha información puede ser mostrada a la persona a quien se deba presentar;

2) Lo dispuesto en el presente artículo no será aplicable a: [...].

ART. 8º—

Variante A:

1) [El órgano o la entidad designada por el Estado promulgante como competente] podrá determinar qué métodos cumplen los requisitos de los artículos 6 y 7.

2) Toda determinación efectuada a tenor del párrafo 1) deberá ser conforme a las normas internacionales reconocidas.

Variante B:

2) Cabrá determinar que uno o más métodos de firma electrónica cumplen los requisitos de los artículos 6 y 7.

3) Toda determinación efectuada al tenor del párrafo 1) deberá ser conforme a las normas internacionales reconocidas.

ART. 9º—

1) Cada titular del dispositivo de creación de la firma deberá:

a) Actuar con diligencia razonable para evitar la utilización no autorizada de su dispositivo de creación de la firma;

b) Dar aviso a quien corresponda sin demora injustificada en caso de que:

i) El titular del dispositivo de creación de la firma tenga conocimiento de que el dispositivo de creación de la firma ha quedado en entredicho; o

ii) Las circunstancias conocidas por el titular del dispositivo de creación de la firma den lugar a un riesgo sustancial de que el dispositivo de creación de la firma pueda haber quedado en entredicho;...

ART. 10.—

- 1) Todo proveedor de servicios de certificación deberá:
 - a) Actuar de conformidad con las declaraciones que haga con respecto a sus prácticas;
 - b) Obrar con la debida diligencia para velar por la exactitud y la integridad de todas las declaraciones pertinentes efectuadas por el proveedor de servicios de certificación que sean de interés para el ciclo vital del certificado o que estén consignadas en el certificado;
 - c) Proporcionar medios razonablemente accesibles que permitan a la parte interesada averiguar:
 - i) La identidad del proveedor de servicios de certificación;
 - ii) Que la persona nombrada en el certificado posee, en el momento pertinente, el dispositivo de firma que se menciona en el certificado;
 - iii) El método utilizado para identificar al titular del dispositivo de firma;
 - iv) Toda limitación de los fines o del valor con los que pueda utilizarse el dispositivo de firma; y
 - v) Si el dispositivo de firma es válido y no está en entredicho;
 - d) Proporcionar a los titulares de dispositivos de firmas un medio para dar aviso de que un dispositivo de firma está en entredicho y asegurar el funcionamiento de un servicio puntual de revocación;
 - e) Utilizar sistemas, procedimientos y recursos humanos fiables para prestar sus servicios.
- 2) Para determinar si ciertos sistemas, procedimientos o recursos humanos son fiables a efectos del apartado e) del párrafo 1), y en qué grado lo son, se tomarán en consideración los siguientes factores:
 - a) Recursos humanos y financieros, incluida la existencia de activo bajo jurisdicción;
 - b) Fiabilidad de los sistemas de equipo y programas informáticos;
 - c) Procedimientos para la tramitación de certificados y solicitudes de certificados y conservación de registros;
 - d) Disponibilidad de información para los [firmantes] [titulares] identificados en certificados y para posibles partes que se fijen de los certificados;
 - e) Regularidad y detalle de la auditoría hecha por un órgano independiente;
 - f) Existencia de una declaración del Estado, un órgano acreditador o el proveedor de servicios de certificación acerca del cumplimiento o la existencia de lo antedicho;
 - g) Estatuto respecto de la jurisdicción de los tribunales del Estado promulgante; y
 - h) Grado de discrepancia entre la ley aplicable a la conducta del proveedor de servicios de certificación y la ley del Estado promulgante.
- 3) Todo certificado dará a conocer:

- a) La identidad del proveedor de servicios de certificación;
- b) Que la persona nombrada en el certificado posee, en el momento pertinente, el dispositivo de firma que se menciona en el certificado;
- c) Que el dispositivo de firma gozaba de validez en el momento en que se expidió el certificado o antes de esa fecha;
- d) Toda limitación de los fines o del valor con los que pueda utilizarse el certificado; y
- e) Toda limitación del alcance o de la cuantía de la responsabilidad que el proveedor de servicios de certificación acepte frente a toda persona.

ART. 11.

Toda parte que confía cargará con las consecuencias jurídicas que dimanen de lo siguiente:

- a) No adoptar medidas razonables, habida cuenta de las circunstancias, para verificar la fiabilidad de la firma electrónica; o
- b) En caso de que la firma electrónica esté refrendada por un certificado, no adoptar medidas razonables, habida cuenta de las circunstancias, para:
 - i) Verificar la validez, la suspensión o la revocación del certificado; y
 - ii) Observar toda limitación relativa al certificado...

ART. 12.

1) Toda persona tendrá derecho a no confiar en la información de un certificado en la medida en que no sea razonable hacerlo.

2) [Para determinar si no es razonable confiar,] [Para determinar si era razonable que una persona hubiese confiado en la información de un certificado,] deberá tenerse en cuenta, en su caso, lo siguiente:

- a) Toda restricción a que esté sujeto el certificado;
- b) Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad del certificado, consultando eventualmente una lista de revocaciones o suspensiones de certificados;
- c) Todo acuerdo o trato que la parte que confía tenga o tuviera en el momento pertinente con el proveedor de servicios de certificación o el suscriptor o todo uso comercial aplicable;
- d) Todos los demás factores pertinentes.

Variante A:

3) Si, dadas las circunstancias del caso, no es razonable confiar en la firma electrónica habida cuenta de los factores indicados en el párrafo 1), la parte que confía asume el riesgo de que la firma no sea válida...

Como se ve, el único precepto que se refiere específicamente a los servicios de certificación y a las obligaciones del proveedor del servicio de certificación es el art. 10 del *Proyecto*. Precisamente este artículo provocó varios debates en el seno del Grupo de Trabajo y, al final, su texto cambió a la forma siguiente:

- 1) El proveedor de servicios de certificación deberá:
 - a) Actuar de conformidad con las declaraciones que haga con respecto a sus normas y prácticas;
 - b) Velar con la debida diligencia porque todas las declaraciones materiales que haga en relación con el ciclo vital del certificado o que estén consignadas en éste sean exactas y cabales;
 - c) Proporcionar medios de acceso razonablemente fácil que permitan al tercero que ha de actuar sobre la base del certificado determinar en éste:
 - i) La identidad del proveedor de servicios de certificación;
 - ii) Que la persona nombrada en el certificado tenía bajo su control el dispositivo de creación de firma al momento de ésta;
 - iii) Que el dispositivo de creación de firma estaba en funcionamiento en la fecha en que se emitió el certificado o antes de ella;
 - d) Proporcionar medios de acceso relativamente fácil que permitan al tercero que ha de actuar sobre la base del certificado determinar, según proceda, en éste o de otra manera:
 - i) El método utilizado para identificar al firmante;
 - ii) Cualquier limitación en los fines o el valor respecto de los cuales pueda utilizarse el dispositivo de creación de firma o el certificado;
 - iii) Si el dispositivo de creación de firma está en funcionamiento y no ha dejado de ser seguro;
 - iv) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el proveedor de los servicios de certificación;
 - v) Si existe un medio para que el firmante dé aviso de que un dispositivo de creación de firma ha dejado de ser seguro;
 - vi) Si se ofrece un servicio de revocación oportuna del certificado;
 - e) Proporcionar un medio para que el firmante avise que un dispositivo de creación de firma ha dejado de ser seguro y cerciorarse de que exista un servicio de revocación oportuna del certificado;
 - f) Utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.

Aunque la variación de este párrafo primero no contiene grandes modificaciones, las variaciones sí son importantes en el detalle. El estado actual del documento espera su revisión para cotejar “la coherencia entre las distintas disposiciones y las versiones en los distintos idiomas”.

Este mismo artículo, además, previene los datos que el propio certificado debe contener y que están identificados con los incisos “a” y “e” del párrafo tercero de dicho art. 10º.

Hay otra breve referencia a las autoridades certificadoras y a los certificados que éstas emiten en el art. 11 modificado, que es precisamente el transcrito en el presente trabajo, concretamente, en

el inciso b). Se refiere a las consecuencias jurídicas que ocasiona el que la firma electrónica se encuentre refrendada por un certificado, puesto que entonces deben verificarse la validez, suspensión o revocación del mismo y reparar en todo tipo de limitaciones propias del documento. También el art. 12 del *Proyecto* se refiere a la confiabilidad de la información del certificado.

21. ALIANZA PARA EL DESARROLLO DE LA RED DE CERTIFICACIÓN Y REGISTRO DE FIRMAS DIGITALES DE LOS NOTARIOS PÚBLICOS MEXICANOS, MÉXICO, 1998

Como se sabe, en nuestro país, la Asociación Nacional del Notariado Mexicano, A. C. celebró un convenio con la empresa INFOSEL. Este convenio es conocido con el nombre de “Alianza para el desarrollo de la red de certificación y registro de firmas digitales de los notarios públicos mexicanos”. Tiene por objeto la prestación del servicio de certificación y registro de firmas digitales. Contiene al principio el índice de los vocablos correspondientes, entre los cuales cabe destacar los términos de *firma digital*, *documento electrónico* y *agente certificador*. Las definiciones más importantes son las siguientes:

Pre-Certificados Digitales: es un documento electrónico firmado digitalmente por un Agente Certificador, en el que se establece la correspondencia de veracidad entre la identidad de un sujeto determinado y la que dice ser su llave pública.

Certificados Digitales: es un documento electrónico firmado digitalmente por la Agencia Certificadora Aplicativa, que certifica tanto la no-duplicidad de un pre-certificado digital, con base en el software de seguridad que al efecto ha sido desarrollado, como la correspondencia de veracidad entre la identidad-licencia de un Agente Certificador y su llave pública, con respecto a dicho pre-certificado.

Agente Certificador: persona física habilitada por la Agencia Certificadora Aplicativa, mediante una licencia de certificación, para que realice el proceso mediante el cual un sujeto determinado acredita su identidad, demuestra su capacidad legal para obligarse, manifiesta su voluntad de que se le certifique la correspondencia de veracidad entre su identidad y la que dice ser su llave pública y firma, además, la declaración de uso de firmas digitales.

Agencia Certificadora Aplicativa: entidad que emite un certificado digital en el que certifica, tanto la no-duplicidad de un pre-certificado digital, con base en el software de seguridad que al efecto ha sido desarrollado, como la correspondencia de veracidad entre la identidad-licencia

cencia de un Agente Certificador y su llave pública, con respecto a dicho pre-certificado.

Agencia Registradora Aplicativa: entidad que registra, para constancia, los certificados digitales emitidos por la Agencia Certificadora Aplicativa y ofrece además, el servicio de consulta sobre el estatus de vigencia o revocación de dichos certificados digitales, mediante la publicación de Listas de Certificados Revocados y/o mediante la emisión de un documento electrónico firmado digitalmente en el que consta esa circunstancia, todo a través de medios electrónicos.

Declaración de Prácticas de Certificación de firmas Digitales: documento tipo en el cual un Agente Certificador manifiesta su interés y voluntad de:

1. Ser habilitado para fungir como Agente Certificador de firmas digitales, una vez cumplidos los requisitos correspondientes;
2. Ejercer la función conferida de conformidad a las normas y procedimientos que al efecto hayan sido definidos por el Comité EDI México y/o por INFOSEL, y
3. Asumir las consecuencias legales y económicas que deriven del ejercicio indebido de dicha función.

La declaración de uso de una firma deberá sujetarse a un documento tipo donde el sujeto interesado manifieste su voluntad de emplear dicha firma digital para la realización de operaciones comerciales, administrativas o jurídicas por medios electrónicos. Esta declaración es recepcionada por un notario agente certificador afiliado a la Asociación, con la licencia previa respectiva, bajo la forma jurídica de una declaración unilateral de voluntad, donde el notario además se cerciora de la identidad del solicitante y expide luego un pre-certificado digital.

El documento se envía inmediatamente a una agencia certificadora (ANNM) que procede a la verificación de su validez y su procedencia por un agente previamente autorizado, hecho lo cual, genera el certificado digital respectivo.

En la última parte del proceso, la agencia certificadora envía a la agencia registradora (INFOSEL) el documento y ésta verifica el registro correspondiente.

Así, el notario que actúa directamente con el usuario entrega finalmente a este último el primer testimonio de la declaración unilateral de voluntad y el certificado digital definitivo.⁴⁹

⁴⁹ El "Manual del Usuario" del Agente Certificador (marzo de 1999, versión 1.1, INFOSEL) describe así el procedimiento:

a) El usuario genera en su computadora sus claves y su requerimiento.

Es innecesario decir, desde luego, que todo este proceso entre el notario público —o corredor, en su caso—, la agencia certificadora y la agencia registradora, tiene lugar en la vía informática y sólo escapa a este medio la presencia física del usuario frente al notario certificador.

22. REFORMAS LEGALES AL CÓDIGO CIVIL FEDERAL, CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES, CÓDIGO DE COMERCIO Y LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR, MÉXICO, 2000

Ha sido expedido el “Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en materia común y para toda la República en materia federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor”.

A) *Código Civil Federal, 1928*

La primera parte de este decreto ha reformado los arts. 1803, 1805, 1811 y ha añadido el art. 1834 *bis* al Código Civil Federal de 1928 en lo que respecta a la incorporación de la posibilidad de “medios electrónicos, ópticos o cualquiera otra tecnología”, equiparando la contratación a la oferta hecha a una persona como si estuviese presente. No se requiere ya de estipulación previa entre los contratantes. Incluso se prevé la intervención de un fedatario público, cuando ello sea necesario, para definir la atribución de la información y la conservación fidedigna de la misma.

b) Con ambos elementos y con los documentos para acreditar su personalidad acude con un Agente Certificador.

c) El Agente Certificador verifica la identidad, imprime la declaración unilateral de la voluntad (DUV) y envía solicitud de registro.

d) La Agencia Certificadora verifica que se trate de un Agente Certificador autorizado y retransmite para su registro.

e) La Agencia Registradora verifica que provenga de una AC autorizada y solicita registro definitivo.

f) La Agencia Registradora Central verifica a los participantes (AgC, AC y AR) y confirma la “no duplicidad” de la clave pública del usuario.

g) La Autoridad Registradora Central envía autorización para registro a través de las AC y AR correspondientes al Agente Certificador.

h) El Agente Certificador recibe respuesta, obtiene firma autógrafa del usuario y le entrega el certificado digital.

i) A partir de ese momento el usuario ya puede realizar transacciones electrónicas.

Ahora bien ¿cuál es la posición de los demás códigos civiles de la República? Desde luego, tendremos que referirnos solamente a los más recientes. Así, por ejemplo, el Código Civil de Veracruz previene la contratación por correo, por teléfono y por telégrafo y se refiere también a la comunicación por “cable, teletipo, radio, telefotografía u otro medio cualquiera similar de comunicación rápida que no consista en la entrega material de documentos autógrafos”. Desafortunadamente, reduce su eficacia a la firma indispensable de los originales respectivos (art. 1744) o al establecimiento de signos convencionales para su identificación.

He aquí un elenco del estado actual de la cuestión. Se consiguen la entidad federativa correspondiente, la fecha de expedición del código y la disposición específica, ya a nivel de comentario o incluso transcribiendo literalmente su texto:

<i>Código Civil</i>	<i>Año de expedición</i>	<i>Artículos</i>	<i>Comentarios o texto:</i>
Quintana Roo	1980	157, 159 y 163	(Se refiere a las comunicaciones postal, telegráfica, telefónica, radiotelefónica y radiotelegráfica. Exige la estipulación previa de las condiciones y firma de los originales.)
Nayarit	1981	1178-1179 y 1184	(Se refiere a las comunicaciones postal telefónica y telegráfica. Exige la estipulación previa de las condiciones y firma de los originales.)
Puebla	1985	1460	“El artículo anterior es aplicable a la oferta hecha por teléfono, radio, télex o cualquier medio de comunicación similar, que permita a la persona que recibe la oferta, contestar inmediatamente.”
Zacatecas	1986	1085 y 1091	(Sólo se refiere a las comunicaciones telegráfica y telefónica. Exige la estipulación previa de las condiciones y firma de los originales.)
Tamaulipas	1987	1271-1272	(Sólo se refiere a las comunicaciones telefónica y epistolar.)
Querétaro	1990	1667-1668 y 1673	(Se refiere a la comunicación postal, telefónica y telegráfica. Exige la estipulación previa de las condiciones y firma de los originales.)
Guerrero	1993	1603-1604	(Se refiere a la comunicación telegráfica, telefónica o por radio, fax, télex y a la correspondencia epistolar.)

<i>Código Civil</i>	<i>Año de expedición</i>	<i>Artículos</i>	<i>Comentarios o texto:</i>
Yucatán	1993	1002	“Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o por otros medios de comunicación mediante los cuales pueda obtenerse respuesta inmediata.”
		1008	“La propuesta y aceptación hechas por telégrafo o radiograma, se equiparan a las hechas por correo, siempre que los originales tengan las firmas de los contratantes o en cualquier otra forma se pruebe su autenticidad.”
Morelos	1994	1675, 1681	(Se refiere a la comunicación telegráfica, telefónica y por telefax. Exige la estipulación previa de las condiciones y firma de los originales.)
Jalisco	1995	1273	“Si la oferta se hace a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por cualquier medio de telecomunicación simultánea.”
Baja California Sur	1996	1710	“Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o por cualquier medio de telecomunicación simultánea.”
		1716	“Cuando exista una oferta al público o en los contratos de ejecución no instantánea, en los de suministro y en los de prestaciones periódicas, es válida y legítima la telecomunicación impresa para considerarse manifestada la voluntad para contratar, siempre que: I. Exista un acuerdo previo entre las partes involucradas para confirmar la voluntad por ese medio o la oferta se haga por medios masivos de comunicación; II. Los documentos transmitidos a través de esos medios, tengan las claves de identificación de las partes, y

<i>Código Civil</i>	<i>Año de expedición</i>	<i>Artículos</i>	<i>Comentarios o texto:</i>
			III. Se firmen por las partes los originales de los documentos donde conste el negocio y tratándose de inmuebles, que la firma sea autenticada por fedatario público.”
Tabasco	1997	1928	“Si el oferente y la persona a quien se hace la oferta estuvieren presentes aquél queda desligado de su oferta si la aceptación no se hace inmediatamente, salvo que el oferente haya hecho la proposición fijando a la otra parte un plazo para aceptar o que este plazo haya sido pactado por ambos. Este artículo es aplicable a la oferta hecha por teléfono o por cualquier otro medio electrónico.”
		1920	“La misma regla establecida en el artículo anterior se aplicará a la oferta hecha por teléfono, radio, télex, o cualquier medio de comunicación similar, que permita al destinatario de la oferta contestar inmediatamente.”
Coahuila	1999	1926	“La oferta y la aceptación hechas por telégrafo, por radiotelegrafía, por fax, o por cualquier otro medio similar, son obligatorias, si los contratantes, con anterioridad habían estipulado, por escrito, esas maneras de contratar y si los originales de las comunicaciones están firmados por el peticionante o por el aceptante, en sus respectivos casos.”

Como se ve, los códigos civiles de Quintana Roo, Nayarit, Zacatecas, Tamaulipas, Querétaro, Guerrero y Morelos (que hacen un total de siete), aun siendo más o menos recientes (es decir, en un rango de 1980 a 1994), sólo hacen referencia a las formas de comunicación que podríamos denominar como tradicionales, es decir, a los modos postal, telefónico, telegráfico y otros. Además, se exige la estipulación previa de las condiciones de contratación y la firma de los originales respectivos.

El caso más extremo de esta pobreza legislativa se encuentra en el código civil de Tamaulipas, que se refiere exclusivamente a las vías de comunicación epistolar y telefónica.

Por otra parte dos códigos civiles, correspondientes a Baja California Sur y Coahuila, efectivamente hacen uso de la expresión

“cualquier medio de comunicación simultánea” o de “respuesta inmediata” o “por cualquier otro medio similar” lo cual, desde luego, implica la comunicación por medios electrónicos.

Por desgracia, ambos códigos continúan exigiendo la estipulación preparatoria (rigurosamente por escrito) y asimismo la firma de los originales respectivos. No obstante, conviene precisar que el código de Baja California Sur reduce esta exigencia a los casos de oferta al público, contratos de ejecución no instantánea, contratos de suministro y a los de prestaciones periódicas.

Los códigos civiles de Puebla, Jalisco, Tabasco y Yucatán (sólo cuatro en total) aceptan sin reservas la contratación por cualquier medio de comunicación “que permita a la persona que reciba la oferta, contestar inmediatamente” o “mediante los cuales pueda obtenerse respuesta inmediata”, sin restringir de alguna forma su uso a la imposición de firmas en los originales o a la celebración de estipulación previa. Ello representa hasta ahora la etapa legislativa más avanzada de la contratación vía electrónica en los códigos civiles provinciales mexicanos.

B) *Código Federal de Procedimientos Civiles, 1942*

En este ordenamiento únicamente se reformó el art. 210-A que dice lo siguiente:

Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

C) *Código de Comercio, 1890*

Por su parte, en este viejo código decimonónico tuvieron lugar importantes reformas. Una de las más trascendentales es la crea-

ción de los folios electrónicos y la informatización del Registro Público de Comercio, el cual funciona a nivel federal.

Por otra parte, se reconocen por primera vez las firmas electrónicas de los servidores públicos, así como de otros usuarios del mismo (notarios, corredores). La Secretaría de Comercio y Fomento Industrial (SECOFI) debe certificar la identificación de las personas autorizadas para firmar electrónicamente y mantener el control para asegurar la confidencialidad de la información. Esta misma secretaría autoriza el acceso a la base de datos del registro. Por último, los comerciantes están obligados, en términos de lo dispuesto en el nuevo art. 49 CCo a:

... conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.

Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

Probablemente la reforma más importante se basa en la inclusión de todo un título en el CCo, denominado “Del comercio electrónico”. En esta parte se reconoce el concepto *mensaje de datos* en los términos siguientes: “Es la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o de cualquier otra tecnología” (art. 89). Se establece expresamente que “Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada” (art. 80). Para el efecto se presume que el momento de recepción de la información se determina como sigue:

...
I. Si el destinatario ha designado un sistema de información para la recepción, ésta tendrá lugar en el momento en que ingrese en dicho sistema, o

II. De enviarse a un sistema del destinatario que no sea el designado o de no haber un sistema de información designado, en el momento en que el destinatario obtenga dicha información.

Para efecto de este Código, se entiende por sistema de información cualquier medio tecnológico utilizado para operar mensajes de datos. (Art. 91.)

Existe la presunción, excepto prueba en contrario, de que el mensaje de datos ha sido recibido cuando el emisor reciba a su vez el acuse correspondiente. Por su parte, también salvo prueba en contrario, se considerará que el mensaje de datos fue expedido en la ciudad donde el emisor tenga su domicilio. Asimismo, el mensaje de datos se tendrá por recibido en la ciudad donde el destinatario tenga su domicilio (art. 94 CCo).⁵⁰

Por último, se modificaron también en forma consecuente disposiciones importantes del procedimiento mercantil, concretamente los arts. 1205 y 1298-A que dicen lo siguiente:

ART. 1205.—Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.

ART. 1298-A.—Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.

¿Puede considerarse que esta forma electrónica satisface la forma escrita? En términos de lo dispuesto en el art. 93 CCo este re-

⁵⁰ Esta disposición debe relacionarse con lo dispuesto en el art. 25 de la Ley 527 colombiana que dice:

“De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:

a) Si el iniciador o destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal;

b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual”.

quisito documental se tiene por satisfecho siempre que el mensaje de datos pueda ser atribuible a las personas obligadas y accesible para su consulta posterior. En este punto se establece expresamente la intervención del fedatario público en los términos siguientes:

...

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige. (Art. 93.)

D) *Ley Federal de Protección al Consumidor, 1992*

La última parte de las reformas mexicanas de junio de 2000 modificó disposiciones importantes del derecho de protección al consumidor. En términos de lo dispuesto en el art. 1º fracción VIII de la LFPC se garantiza la efectiva protección del consumidor en las transacciones electrónicas, incluso a través de códigos de ética por parte de los proveedores, cuya adopción sería voluntaria y espontánea. Estos códigos de ética tendrían como objetivo la incorporación de los principios previstos en la LFPC para las transacciones electrónicas celebradas con los consumidores. Se prevé concretamente el cumplimiento de los siguientes puntos (art. 76 bis):

- a) Utilización de la información en forma confidencial.
- b) Información de las características de los elementos técnicos disponibles para la seguridad y confiabilidad de la información.
- c) Proporcionar datos personales del proveedor.
- d) Evitar prácticas comerciales engañosas.
- e) Información sobre los términos, condiciones, costos y cargos del producto o servicios.
- f) Información respecto de la cantidad y calidad de los productos.
- g) Información sobre las estrategias de venta o de publicidad, especialmente con referencia a niños, ancianos y enfermos.

Por último, las infracciones consignadas en estas reformas pueden ser sancionadas en términos de lo dispuesto en el art. 128 LFPC hasta por una multa equivalente a 2,500 veces el salario mínimo

general vigente (SMGV) en la ciudad de México, es decir, \$95 mil pesos mexicanos (aproximadamente \$10 mil USD).

CONCLUSIONES

Es sumamente difícil ofrecer un panorama general y exhaustivo del estado actual del comercio electrónico y de las autoridades certificadoras en virtud de los cambios tan rápidos que se producen en este campo. Sí es posible, sin embargo, dar noticia de los últimos adelantos en general, porque se advierte una gran uniformidad en la legislación respectiva.

Así, por ejemplo, Dinamarca tiene un proyecto sobre firmas digitales con esquemas de autorización tácita y expresa para las autoridades certificadoras con requisitos más o menos rigurosos según el caso. Finlandia se encuentra trabajando específicamente en el tema de la responsabilidad de estas autoridades y sobre la posibilidad de que empresas particulares y organizaciones extranjeras puedan participar de esta cualidad. En Alemania operan ya organismos certificadoros de carácter privado, bajo el esquema de la Ley de Firmas Digitales de ese país. En este país operan también los denominados *notarios públicos electrónicos*.

Por su parte, en Irlanda existe un sistema legal de acreditación voluntaria de entes certificadoros, a quienes se imputa responsabilidad por la información contenida en sus certificados. En Malasia se hacen esfuerzos en el mismo sentido, bajo el marco de la *Digital Signature Act* de 1997, pero hasta la fecha los entes certificadoros sólo existen a nivel de plan piloto y sin ánimo de lucro.

En Holanda, sin embargo, opera ya un servicio de “notario público digital” en línea. En Inglaterra existe un conflicto con el resto de la Unión Europea, precisamente en el punto relativo al carácter de las autoridades certificadoras licenciadas, puesto que la legislación que se prepara únicamente reconocería el carácter legal de estas últimas. Sin embargo, la *Electronic Signature Directive* de la Unión Europea no distingue entre autoridades licenciadas y no licenciadas.

Apenas el 29 de febrero de 2000 la Asamblea Nacional francesa discutió un proyecto de ley con relación a la reforma de las pruebas legales en el campo de las nuevas tecnologías informáticas y especialmente de las firmas electrónicas. El proyecto consta de apenas unos cuantos preceptos que modifican los arts. 1316-1317 y 1326 del *Code Civil*. Se refieren a la prueba de las obligaciones y a los títulos auténticos.

En los Estados Unidos, el panorama legislativo se encuentra muy fraccionado, en virtud del régimen federal y la gran evolución tecnológica del país.

En el transcurso de estos pocos años, California, Georgia, Nuevo México, Massachusetts, Illinois, Oregon, Virginia, Washington y otros estados han expedido (o están en proceso de expedir) leyes sobre comercio electrónico y firmas digitales, definiendo los términos respectivos, instaurando autoridades certificadoras, regulando las cualidades de los licenciarios y consignando previsiones para eventuales falsificaciones y aumento de la confiabilidad del público en las firmas verificadas por medios electrónicos.

Algunas de estas leyes pueden ser más o menos parecidas entre sí. Sin embargo, debe tenerse aquí muy presente la declaración emitida por el presidente Bill Clinton de que no resulta posible, por ahora, pensar en una ley uniforme en todo el ámbito federal de la Unión, a pesar de los esfuerzos de la *National Conference of Commissioners on Uniform State Laws* (NCCUSL).

En la red pueden encontrarse al respecto páginas sumamente interesantes como la de *The Digital Signature Law Survey*, a cargo de *The Dutch National Programme on IT and Law* y bajo la responsabilidad de Simone van der Hof (la dirección electrónica aparece al final de este ensayo). Este documento se refiere al estado actual de la legislación sobre firmas digitales a nivel mundial. Sus fuentes documentales se remontan al material recolectado en la propia red, publicaciones en soporte papel tradicional e incluso a comunicaciones personales sostenidas por la autora. La última versión de que dispongo es la 3.9 correspondiente a abril de 2000. El documento contiene un total de ochenta y ocho referencias que comprenden muchos países y organismos oficiales.

Por otra parte, la literatura especializada que se ha producido al respecto resulta abundante y de gran originalidad, dada la magnitud y complejidad del problema. Hay publicaciones específicamente diseñadas como la *Revista Electrónica de Derecho Informático* (REDI) que trata temas puntuales no solamente de comercio electrónico, sino de tecnología informática en general y cuestiones relacionadas.

¿Cuáles son, en líneas generales, las funciones de estas Autoridades Certificadoras? Un breve elenco de ellas debería comprender por lo menos la compilación, el registro, la actualización y la publicación de claves digitales, así como las medidas de seguridad

necesarias para preservar su inalterabilidad, su recuperación y su atribución personal.

Esta función básica, al propio tiempo, permitiría el acceso oportuno a otras funciones de carácter secundario consistentes en servicios de prelación registral, documentación del proceso y mediación y arbitraje entre las partes.

¿Qué entidades podrían ser merecedoras de semejante función? Pues, como se ve, se involucran al mismo tiempo complejas cuestiones tanto de orden técnico cuanto de confiabilidad y certeza. Así, el rango de opciones cubre una amplia variedad de personas individuales y jurídicas que pueden asumir la función: *international notarial practitioners*, *international attorney-notaries*, notarios públicos del sistema latino, corredores, registradores, conservadores de la propiedad, funcionarios oficiales, bancos, cámaras de comercio, *escrow agents*, casas de bolsa, *cybernotaries*, *civil-law notaries*, ministros de fe, proveedores de equipos electrónicos, notarios públicos electrónicos, fedatarios particulares juramentados, *malls* especializados, asociaciones de comercio electrónico, empresas productoras de *software*, gerentes de sitios internet (*website's postmasters*) compañías de seguros, secretarías de estado, oficinas postales, correos paralelos (DHL, UPS, FEDEX), etc.

Aun siendo sumamente variado el panorama legislativo acerca de las autoridades de certificación, puede en resumen advertirse un marco común que les presta cierta unidad. En general, resulta necesario el establecimiento de una autoridad gubernamental que ejecute labores de vigilancia y supervisión, así como de registro y conservación de los certificados expedidos. Son bastante similares las características que deben observar estos certificados. Además, debe ajustarse su vigencia a un cierto plazo determinado, que desde luego puede variar en los casos concretos. Este es uno de los puntos más vulnerables del certificado y no es casual, por tanto, que se establezcan disposiciones importantes para salvaguardar su vigencia, suspensión y cancelación bajo estrictos controles de archivo y publicidad. Por lo general tiene un costo, el cual muchas veces depende del grado de confiabilidad y responsabilidad que finalmente asuma la entidad certificadora.

El análisis comparativo de las entidades de certificación arroja resultados sumamente valiosos que enriquecen desde luego las posibilidades de esta figura y la consecuente intervención notarial. Un ejemplo de ello lo tenemos en el protocolo notarial electrónico chileno y especialmente en la exclusividad de los notarios para

actuar como autoridades certificadoras. Por otra parte, ya hemos visto que la *Electronic Transactions Act* de Alabama dedica un capítulo especial a la figura de la *notarization*. Ésta consiste en la práctica de escrituras públicas, reconocimientos, certificaciones y declaraciones bajo fe de las firmas electrónicas de personas autorizadas para ejecutar tales actos, siempre y cuando la firma pueda ser reputada como lógicamente asociada con la persona que la expide o la asume como propia.

Como se sabe, cada certificado debe ser expedido a nombre del suscriptor del servicio. Sin embargo, la ley alemana incorpora una importante novedad cuando previene la posibilidad del registro de seudónimos en el lugar del nombre verdadero del solicitante.

En el sistema de promoción del comercio electrónico japonés, he mencionado la figura del notario electrónico actuando a través de centros específicos denominados precisamente Centros Notariales Electrónicos. Pero las innovaciones no se reducen exclusivamente a esta única figura. El propósito de la creación de estos centros se centra más bien en la disponibilidad de servicios amplios y cómodos para el usuario, como lo demuestra la posibilidad de su establecimiento en tiendas de consumo, compañías de seguros, asociaciones comerciales, proveedores de servicios electrónicos, grandes centros comerciales, etc.

He destacado también en el curso de este trabajo la participación abierta del sector empresarial en régimen estricto de libre competencia, según pasa en España. Por otra parte, la mayoría de las legislaciones avalan, apenas con mínimas reservas, la homologación de los certificados de firmas digitales emitidos por entidades de certificación extranjeras, lo cual de algún modo reduce la distancia que nuestros países latinoamericanos mantienen en relación con el ámbito económico de la Unión Europea.

Es importante considerar que los procedimientos de seguridad y verificación digital puedan encontrarse abiertos al examen público y en este sentido ya hemos visto que en Singapur existe un sitio especial en la red bajo supervisión constante de la autoridad controladora (*Controller's Internet website*).

¿Qué sucede en el caso de que las entidades de certificación actúen bajo la forma de personas morales o jurídicas? El solo cambio de directivos o de funcionarios responsables plantea, en la práctica, una serie de problemas que es necesario resolver. Así, en Singapur se exige la obligación de las autoridades de certificación de informar rigurosamente acerca de cualquier cambio en sus fun-

cionarios en el breve plazo de tres días a partir de la asunción del cargo. En relación con la propia naturaleza jurídica de esas autoridades ya hemos visto en algún caso la exigencia expresa de que se trate tan sólo de sociedades por acciones, según refieren las leyes italianas. En contrapartida, Chile admite también la forma de sociedades personales. Además, es sumamente interesante la facultad que se concede a las propias entidades para elaborar los reglamentos que definan las relaciones con el suscriptor y la forma de la prestación del servicio, así como los manuales técnicos de procedimiento.

En el caso de Argentina deseo destacar particularmente la posibilidad de que la autoridad certificante licenciada pueda admitir en un certificado cierta información que no haya sido verificada y que, por tanto, no pueda constar en forma fehaciente en los registros de la licenciada. Es cierto que la responsabilidad se soslaya con la simple advertencia de indicar, sin lugar a dudas, tal circunstancia. Sin embargo, esta disposición puede representar en el futuro un punto importante de vulneración en la confiabilidad de los entes certificantes.

Por otra parte, disposiciones específicas en leyes alemanas toman con reservas el almacenamiento de la clave privada por parte del certificador a fin de asegurar, por todos los medios posibles, la confiabilidad de la misma; mientras tanto, las leyes argentinas insisten expresamente en la obligación de la autoridad certificante para mantener el control de dicha clave e impedir su divulgación.

¿Qué decir respecto de las tecnologías? La mayoría de las legislaciones consultadas adopta posiciones muy cautas acerca de la adopción de algún modelo tecnológico particular. Sin embargo, no es éste el ejemplo de la ley de Texas que específicamente patrocina la adopción oficial de los sistemas *Public Key Cryptography* y *Signature Dynamics*.

Debe existir un sistema de seguridad registral consecuente con las necesidades de salvaguarda de la confiabilidad de las claves y efectiva publicidad de los certificados y de las prácticas de seguridad. Pues bien, la ley pionera de Utah previene la posibilidad de que no necesariamente deba publicarse el certificado emitido en los archivos oficiales, pues las partes —autoridad certificante y suscriptor— pueden convenir en sentido contrario.

Por último, no deben olvidarse las repercusiones que todo este tema tiene en otros puntos específicos, por ejemplo, lo relaciona-

do con la Convención de La Haya de 1961 relativa a la imposición de apostillas en los documentos de circulación internacional, caso éste en el cual habría quizás necesidad de crear la apostilla electrónica.

Sea como fuere, la contratación electrónica mantiene ciertos límites que no pueden todavía ser rebasados, al menos en el estado actual de nuestra tecnología informática. ¿Cuáles son estos límites? Ya se ha visto en el curso de la investigación que algunas leyes electrónicas limitan el alcance de este tipo de contratación especificando que ella no es aplicable a testamentos, escrituras públicas (la Directiva CE-97 excluye expresamente los contratos inmobiliarios), actos solemnes, títulos de crédito, poderes, garantías inmobiliarias, documentos electorales, etc. A este tipo de negocios deben sumarse algunas pocas operaciones bancarias, contratos de seguro, mutualidades y certificaciones notariales de visu (respecto de hechos solamente percibidos por los sentidos, como certificados de salud o supervivencia, actas de presencia, entrega de documentos, de dinero o de efectos, exhibición de objetos, requerimientos, notificaciones, interpelaciones, actas de notoriedad y daciones de fe en general). Sin embargo, debe recordarse aquí la novedosa previsión del proyecto chileno para la aplicación de firmas electrónicas en el endoso de documentos mercantiles, tales como facturas, letras de cambios, pagarés, pólizas de seguros, documentos de embarque y valores negociables.

BIBLIOGRAFÍA

I. Obras generales

- BARRIOS GARRIDO, Gabriela, MUÑOZ DE ALVA, Marcia y PÉREZ BUSTILLO, Camilo, *Internet y derecho en México*, Mc Graw-Hill, México, 1998.
- BETLEM, Gerrit y otros, *Towards a European civil code*, Martinus Nijhoff Publishers, Dordrecht, 1994.
- MÉJAN, Luis Manuel, "La contratación por medios electrónicos de operaciones del sistema financiero mexicano", en: *Revista de Derecho Privado*, N° 21, 1996, Mc Graw-Hill, UNAM, México, 1996, pp. 29 y ss.
- PAIÑO MANFER, Ruperto, *Contratación internacional*, BANCOMEXT, México, 1995.
- ZWEIGERT, Konrad and KOTZ, Hein, *An introduction to comparative law*, Clarendon Press Oxford, 1994.

II. Obras específicas

- ARREDONDO GALVÁN, Francisco X., "El notario de tipo latino ante los desafíos de la informática", en: *Revista de Derecho Notarial*, N° 110, ANNM, A. C., México, 1997, pp. 119 y ss.

- BARASSI, Theodore, "El Cybernotary: ¿clave para registrar y certificar los servicios del comercio electrónico internacional?", Conclusiones de la IX Jornada Notarial de América del Norte, Centroamérica y el Caribe, en: *Boletín de la Asociación Nacional del Notariado Mexicano, A. C.*, N° 4, México, 1998.
- , "The cybernotary: Public Key Registration and Certification Services for International Electronic Commerce", en: *Notarius International*, No. 3, The Hague, 1996, pp. 105 y ss.
- BOLAS ALFONSO, Juan, "Les contrats négociés à distance et la portée de la directive 97/7/CE du Parlement Européen et du conseil concernant la protection des consommateurs", en: *Notarius International*, N° 3, The Hague, 1997, pp. 102 y ss.
- DEVOTO, Mauricio, "El comercio electrónico y la firma digital", Conclusiones de la IX Jornada Notarial de América del Norte, Centroamérica y el Caribe, en: *Boletín de la Asociación Nacional del Notariado Mexicano, A. C.* N° 4, México, 1998.
- FAERDER, Charles, "Notarialización electrónica", en: *Revista Internacional del Notariado*, N° 96, Buenos Aires, 1998, pp. 189 y ss.
- FUENTE, Juan Ángel de la, "La contratación electrónica, la criptografía y la firma digital", en: *Revista Internacional del Notariado*, N° 96, Buenos Aires, 1998, pp. 173 y ss.
- HACKENBUCHNER, Wolfgang, "Nacimiento del ciber-notario", en: *Revista Internacional del Notariado*, N° 94, Buenos Aires, 1997, pp. 102 y ss.
- KENNAIR, William, "The Concept and Development of the Cybernotary", en: *Notarius International*, N° 3, The Hague, 1996, pp. 121 y ss.
- LAMBERT, Jean y CASSIUS, Robert, "El secreto profesional y las comunicaciones electrónicas", en: *Revista Internacional del Notariado*, N° 94, Buenos Aires, 1997, pp. 162 y ss.
- MÁRQUEZ GONZÁLEZ, José Antonio, "Marco legal de la contratación electrónica", en: *Revista de Derecho Notarial*, N° 113, ANNM, A. C., México, 1999, pp. 39 y ss.
- , "Civil-Law Notary, Florida, 1998" en: *Revista Notarial del Colegio de Notarios del Estado de Veracruz*, año 2, N° 4, Xalapa, 1999, pp. 51 y ss.
- , "Del barro cocido a la memoria electrónica", en: *Revista Internacional del Notariado*, N° 99, Buenos Aires, 2000, pp. 150 y ss.
- , "Ley del notario de derecho civil del estado de Florida", en: *Revista de Derecho Notarial*, N° 114, ANNM, A. C., México, 1999, pp. 26 y ss.
- , "La contratación electrónica en los códigos civiles", en: *Boletín Banamex*, México (en prensa).
- , "El notariado en Italia", en: *Revista de la Facultad de Derecho de México*, tomo XLV, no. 199-200, UNAM, México, 1995, pp. 231 y ss.
- MICCOLI, Mario, "Comercio telemático: una nueva realidad en el campo del derecho", ponencia presentada en Conclusiones de la IX Jornada Notarial de América del Norte, Centroamérica y el Caribe, en: *Boletín de la Asociación Nacional del Notariado Mexicano, A. C.*, N° 4, México, 1998.
- , "Cybernotary", en: *Revista Internacional del Notariado*, N° 91, Buenos Aires, 1996, pp. 128 y ss.
- , *La sicurezza giuridica nel commercio elettronico*, tesis de licenciatura, Universidad de Pisa, 1995.

- MURRIETA, Katia, "La contratación por vía electrónica", Conclusiones de la IX Jornada Notarial de América del Norte, Centroamérica y el Caribe, en: *Boletín de la Asociación Nacional del Notariado Mexicano*, A. C., N° 4, México, 1998.
- NIÑO DE LA SELVA, José de Jesús, "Red de certificación digital" en: *Boletín de la Asociación Nacional del Notariado Mexicano*, A. C., N° 10, México, 1998, pp. 38 y ss.
- "Notaries and Electronic Legal Transactions: Preliminary Advice", Annual General Meeting of the Members of the *Koninklijke Notariële Broederschap* (KNB), Breda (Netherlands), 4 october 1996.
- NÚÑEZ PALOMINO, Germán, "La identificación de las personas naturales por vía electrónica como factor de contratación", Conclusiones de la IX Jornada Notarial de América del Norte, Centroamérica y el Caribe, en: *Boletín de la Asociación Nacional del Notariado Mexicano*, A. C., N° 9, México, 1998, pp. 24 y ss.
- ORTIZ PELLEGRINI, Horacio Arturo, "Comercio electrónico", Conclusiones de la IX Jornada Notarial de América del Norte, Centroamérica y el Caribe, en: *Boletín de la Asociación Nacional del Notariado Mexicano*, A. C., N° 9, México, 1998, pp. 24 y ss.
- PRADA, Vicente de, "El documento informático: su encaje en el sistema del notariado latino" (primera parte), en: *Boletín de la Asociación Nacional del Notariado Mexicano*, A. C., N° 5, México, 1998, pp. 4 y ss.
- , "El documento informático: su encaje en el sistema del notariado latino" (segunda parte), en: *Boletín de la Asociación Nacional del Notariado Mexicano*, A. C., N° 6, México, 1998, pp. 31 y ss.
- RIVERA FARBER, Octavio, "La contratación electrónica", en: *Revista de Derecho Notarial*, N° 110, ANNM, A. C., México, 1997, pp. 115 y ss.
- SIRI GARCÍA, Julia, "La intervención notarial en el documento informático", Conclusiones de la IX Jornada Notarial de América del Norte, Centroamérica y el Caribe, en: *Boletín de la Asociación Nacional del Notariado Mexicano*, A. C., N° 4, México, 1998.
- TASSÉ, Roger, and LEMEUX, Kathleen, *Consumer Protection Rights in Canada in the Context of Electronic Commerce*, Office of Consumer Affairs, Quebec, 1998.

III. Legisgrafía

- Decreto 427/98 de Firmas Digitales para la Administración Pública Nacional, Argentina, 1998
- Digital Signature Act*, Malasia, 1997
- Digital Signature Act*, Hong Kong, 2000
- Digital Signature Guidelines* (ABA), USA, 1996
- Digital Signature*, Texas, 2000
- Decreto N° 81. Regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado, Chile, 1999
- Electronic Commerce Promotion Council of Japan*, 1998
- Electronic Records and Signatures Act*, Massachusetts, 1998
- Electronic Signature Directive*, Unión Europea
- Electronic Transactions Act*, Alabama
- Electronic Transactions Act*, Singapur, 1998
- Electronic Transactions (certificación Authority) Regulation*, Singapur, 1999

- Florida Electronic Signature Act*, Florida, 1996
Illinois Electronic Commerce Security Act, Illinois, 1999
Legge 15 marzo 1997, n. 59, Italia
Ley 527 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones, Colombia, 1999
Ley de Firmas Digitales, Puerto Rico, 1998
Ley de Firmas y Certificados Digitales, Perú
Ley Modelo sobre Comercio Electrónico (UNCITRAL), 1996
Projet de Loi, 29 février, 2000, France
Proyecto de Ley sobre Documentos Electrónicos, Chile
Proyecto de Régimen Uniforme para las firmas electrónicas (UNCITRAL), 1996
Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, España, 1999
Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica, España, 2000
Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, Italia, 1997
Teledienstegesetz (TDG), Signaturgesetz (SiG), Alemania, 1997
Uniform Electronic Transactions Act, Massachusetts, 1999
Utah Digital Signature Act, Utah, 1995
Utah Notaries Public Reform Act, Utah, 1998

IV. Direcciones electrónicas

- ABA *Section of Science and Technology CyberNotary Committee*
www.abanet.org/scitecn/ec/cn/cybernote.num
California, *Digital Signature Regulations*, 1998
www.ss.ca.gov/digsig/regulations.htm
Consiglio Nazionale del Notariato. CNN Notizie
<http://www.notariato.it/ciao.pdf>
Consumer Protection Rights in Canada in the Context of Electronic Commerce
www.strategis.ic.gc.ca/SSG/ca01031e.html
Decreto no. 81. Regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado, Chile, 2000
www.modernizacion.cl/firm_doc_elect/index.htm
Electronic Authentication, New México, 1996
www.softwareindustry.org/issues/nmdsregsm_
Electronic Commerce in Florida. Report to the Joint Legislative Committee on Information Technology Resources, Florida Department of State.
www.leg.state.fl.us/citizen/documents/statutes/1998/ch0117/tit10117.htm
Electronic Commerce Canada
<http://www.ecc.ca/About/Description.html>
Electronic Records and Signatures Act, Massachusetts, 1998
www.magnet.state.ma.us/itd/legal/mersa
Frequently asked questions regarding digital signatures
www.commerce.state.ut.us/web/commerce/digsig/dsfaq.htm
Florida Electronic Signature Act, 1996

www.leg.state.fl.us/citizen/documents/statutes/index.html
Georgia Electronic Records and Signatures Act, 1997
www.cc.emory.edu/BUSINESS/digital_signature_draft
Illinois Electronic Commerce Security Act, 1999
www.ag.state.il.us/resource/cecc/cecc2.htm
The Digital Signature Law Survey, 2000
file:///A:digitalsignatureindice.htm,
Orden de 21 de febrero de 2000, por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica
<http://vlex.com/es/boe/buscar>
Oregon Electronic Signature Act, 1997
www.cbs.state.or.us/external/dfcs/digsig.
Revista Electrónica de Derecho Informático (REDI)
<http://derecho.org/redi/index.cgi>
Uniform Electronic Transactions Act, Massachusetts, 1999
www.magnet.state.ma.us/id/legal/
Utah Digital Signature Act, 1995
www.commerce.state.ut.us/web/commerce/digsig/act
Utah, Notaries Public Reform Act, 1998
www.le.state.ut.us/~code/TITLE46/46_01
VeriSign
Wysiwyg://2/http://www.verisign.com/
Virginia Senate Bill
Virginia House Bill
www.mbc.com/legis/virginia.html
Washington, *Digital Signature Law*, 1997
www.jmslaw.com/0005