La Ley de Firmas Digitales de Puerto Rico y el desarrollo del notario cibernético

Antonio J. Colón García*

Introducción

El mundo en que vivimos se encuentra en un constante cambio debido a la avanzada tecnología que domina las comunicaciones. Un elemento muy importante dentro de este campo es el comercio electrónico. El comercio electrónico ha sido de vital importancia en el Derecho internacional. Mediante la utilización de éste, se han trascendido las fronteras internacionales de una forma nunca antes imaginada. La espina dorsal del comercio electrónico es la firma digital, ya que mediante la utilización de ésta se le otorga validez jurídica al negocio.

La creciente sustitución de la escritura en la vida jurídica y de los negocios ha hecho que las ventajas y riesgos típicos de las declaraciones realizadas por vía electrónica sean evidentes para todo el mundo. En efecto, el documento electrónico, si bien de una naturaleza menos tangible que el documento en papel, no ha perdido por completo su esencia corporal. Permite su reproducción a voluntad y ser transportado en cuestión de segundos sin importar la distancia. Es volátil y puede ser manipulado fácilmente. En tanto que el emisor de la declaración no resulte visible, la información también puede ser fácilmente manejada. Por lo expuesto, el destinatario de una declaración electrónica no puede confiar en la identidad de su interlocutor ni en la autenticidad del texto que le ha sido transmitido.

Vistas las considerables ventajas económicas que su utilización implica, se tiende a dejar de lado por un instante los inconvenientes planteados para reconocer que las garantías de seguridad tecnológicas y jurídicas disponibles son superiores a aquellas que se aceptan para el documento de papel. Sin embargo, dado la naturaleza revolucionaria de esta tecnología, se deben tomar medidas tendientes a lograr su perfección,

---

*Estudiante de segundo año y miembro del Cuerpo de Investigadores, Redactores y Correctores de la Revista de Derecho de la Pontificia Universidad Católica de Puerto Rico. Quiero agradecer la cooperación brindada por el Profesor Miguel Álvarez Pons por su ayuda en la corrección de este artículo.

a fin de evitar que estas herramientas tan ventajosas puedan ser destruidas por la crítica.

A nivel internacional, se han aprobado diversas leyes otorgándole a la firma digital el mismo efecto de la firma de puño y letra.[1] Para salvaguardar la integridad de esta firma y evitar todo tipo de fraude en cuanto a ésta, se ha diseñado una tecnología que estipula unos patrones de seguridad que ofrecen la confiabilidad de la misma. Esta tecnología se ha denominado "criptosistema asimétrico".

La necesidad de regular las transacciones electrónicas utilizando firmas digitales, ha dado paso a que la labor tradicional del notario sufra una metamorfosis. El notario que esté dispuesto a trabajar con este tipo de transacciones tiene que estar altamente capacitado en el manejo de las computadoras y en el funcionamiento de criptosistemas asimétricos. Para que esta tecnología trabaje de forma adecuada, debe introducirse un paralelo de medidas técnicas estandarizadas, una legislación especial y una infraestructura de seguridad. El 7 de agosto de 1998 se aprobó la Ley 188 de Firmas Digitales de Puerto Rico y con ésta se abrió una brecha en el campo de la notaría. Esta Ley todavía no ha sido implementada, la misma reconoce a la rúbrica digital, que se realiza a través de claves de algoritmo, el mismo efecto legal que se reconoce en nuestro ordenamiento a la firma de puño y letra. Esto abre un nuevo campo de estudio para el notario puertorriqueño. Todo esto se debe al interés del Estado en fomentar la industria a través del comercio electrónico y a la necesidad de proveer cierto grado de confiabilidad a las transacciones hechas por estos medios.

El propósito de este artículo es estudiar el funcionamiento de las transacciones electrónicas utilizando firmas digitales, las cuales están reguladas por la Ley de Firmas Digitales de Puerto Rico. Se pretende analizar cuál es el impacto de este tipo de legislación en el desarrollo del notario cibernético de tradición civilista. Para que este análisis sea posible, es necesario estudiar tres factores claves. Primero, cuáles son las técnicas de seguridad estandarizadas. En cuanto a este aspecto, se estudiarán los criptosistemas asimétricos y simétricos. El segundo, es el estudio de la legislación pertinente al asunto. En nuestro caso en particular, estudiaremos la Ley de Firmas Digitales de Puerto Rico. Por último, se estará tratando la infraestructura de seguridad que otorga la

[1] Ley de Firmas Digitales de Puerto Rico de 1998, art. 1, 3 L.P.R.A. §1031 (Supl. 1999).

validez jurídica al documento electrónico. En cuanto a este aspecto, se tocará el tema de las autoridades certificadoras y la posibilidad de que el notario pueda ejercer las funciones relacionadas a éstas.

I. Trasfondo e historial legislativo

A. El Comercio electrónico

La difusión masiva de mecanismos que procuran brindar seguridad a la transmisión de información entre computadoras, surge fundamentalmente a partir del desarrollo del comercio electrónico en redes abiertas, como lo es la Internet. El éxito del comercio electrónico se basa en la aparición de un mercado global (la red), en el cual el contacto físico ha sido relegado y reducido a su mínima expresión. El comercio electrónico consiste en la transformación de las transacciones y procesos basados en papel en un proceso digital en que la palabra, anteriormente impresa en papel, es reemplazada por el lenguaje de las computadoras. Para que dicho mercado global se convierta en un medio apropiado para el comercio, debe existir una forma de asegurar que los emisores y receptores de dicho lenguaje puedan ser identificados con cierto grado de certeza y que la información transmitida no sufra alteraciones.

Para comprender la clase de solución que se necesita, a efectos de implementar una infraestructura global de información, es indispensable entender el tipo de tráfico comercial que desea transportarse por las redes. El comercio minorista es una pequeña parte del futuro del comercio digital. Existe un espectro de servicios (legales, financieros, de salud) que pueden ser ofrecidos más eficientemente con la ayuda de las redes abiertas. Para que los sistemas abiertos puedan ser utilizados para transportar esta clase de información, es indispensable poder identificar las personas que participan en las comunicaciones, independientemente del lugar físico utilizado. La tecnología requerida para lograr la seguridad a que se ha hecho referencia ya existe en la forma de la firma digital, basada en criptosistemas asimétricos.

B. ¿Qué son criptosistemas?

Para darle seguridad a la información, es necesario utilizar técnicas criptográficas. Encriptar significa tornar un documento legible en uno

ilegible de acuerdo a una fórmula matemática.[2] Obviamente, encriptar un documento tiene sentido únicamente si es posible desencriptarlo, o sea, volver a recuperar el texto original a base del texto cifrado. Este proceso de encriptar y desencriptar carecería de utilidad si fuera igual de fácil para todos desencriptar el documento. En realidad es extremadamente difícil desencriptar un documento, conllevaría hasta millones de años de análisis por las computadoras más avanzadas. Esto es, claro, a menos que se conozca la clave. Disponer de la clave torna la tarea de desencriptar un documento en una tarea prácticamente trivial, siempre y cuando la clave utilizada para desencriptar sea la misma que la utilizada para encriptar el documento original. Las técnicas de encriptado que funcionan de esta manera se denominan *simétricas* puesto que se requiere la misma clave para desencriptar el documento como para encriptarlo.[3] Para que este sistema funcione, debe mantenerse secreta la clave o, de lo contrario, cualquiera podría tener acceso al documento.

Supongamos que obtenemos la información digital de los documentos previamente escaneados, pero, antes de grabar el CD-ROM, encriptamos toda esa información con una clave secreta. Luego, si un individuo intenta fraguar el documento, no lo va poder hacer, ya que no lo podrá leer. Más aun, si alterara de forma alguna el documento, el desencriptado ya no funcionaría debido a que el texto alterado diferiría del texto encriptado originalmente y la clave secreta ya no tendría ninguna utilidad. El problema entonces sería que, ni el individuo malintencionado ni los usuarios legítimos podrán leer estos documentos digitales. La solución sería facilitar la clave secreta a los usuarios legítimos para poder acceder a los documentos, pero, entonces, la clave secreta ya no sería secreta. Es más, el usuario legítimo de hoy puede convertirse en el individuo malintencionado de mañana. Una vez que conoce la clave secreta, la cual ya no sería secreta, puede desencriptar los documentos, alterarlos, volver a encriptarlos con la misma clave y grabar un nuevo CD-ROM para sustituir al original. Esta necesidad de tener que divulgar la clave secreta vulnera al encriptado de clave simétrica y lo vuelve inutilizable para otorgarle seguridad jurídica al documento electrónico.

C. Criptosistema asimétrico

---

[2] F. LAWRENCE STREET, LAW OF THE INTERNET 15 (1998).

[3] Miguel A. Monjas, *Usos de criptografía en mecanismos de pago* (visitado el 21 de octubre de 1999) <http://www.dat.etsit.upm.es/~mmonjas/pago/cripto.html>.

Para resolver este problema, los criptógrafos diseñaron métodos que no requieran divulgación de la clave secreta. Estos métodos utilizan una clave para encriptar el texto original y otra clave, diferente de la primera, para desencriptar el texto cifrado y recuperar así el texto original. Por utilizar dos claves diferentes para encriptar y desencriptar estos métodos se denominan criptosistemas asimétricos.[4] A manera de ejemplo, supongamos que tenemos las claves X y Z. Este método tiene la propiedad de que, si el texto original se encripta con la clave X, tiene que ser desencriptado con la clave Z, mientras que, si el texto original se encripta con la clave Z, tiene que ser desencriptado con la clave X. Como una de las dos claves se publica, mientras que la otra clave se mantiene privada, las claves se denominan pública y privada, respectivamente. Esto significa que un documento encriptado con una clave privada puede ser únicamente desencriptado con la correspondiente clave pública, mientras que un documento encriptado con una clave pública puede ser únicamente desencriptado con la correspondiente clave privada.

Los criptosistemas asimétricos se han desarrollado en los Estados Unidos desde la década del setenta, tanto en el sector público como en el privado.[5] Las agencias gubernamentales que intervienen en su desarrollo son la NSA (*National Security Agency*), que es el seno de los criptosistemas con fines de espionaje, en forma conjunta con el NIST (*National Institute for Standards and Technology*), que determina los estándares de firma digital a utilizarse en el gobierno y por los proveedores del mismo y que ha promulgado el DSS (*Digital Signature Standard*) en base a los criptosistemas asimétricos. La CCITT (*Consultative Committee on Internacional Telecommunications and Telegraphy*), el ISO (*International Standards Organization*), ambos en Ginebra, Suiza y el PKCS (*Public Key Criptography Standards*, un consorcio de *Apple, Microsoft, Digital, Lotus, Sun y el Massachusetts Institute of Technology*), han implementado todos estándares a base de los criptosistemas asimétricos.[6]

---

[4] *Véase* Brad Biddle, *Public Key Infrastructure and Digital Signature Legislation: Ten Public Policy Questions,* 2 CYBER. LAW 7 (1997).

[5] William A. Hodkowski, *The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law,* 13 COMPUTER & HIGH TECH. L.J. 217 (1997).

[6] Gus Hosein, *Consultation and Contemplation: What Has Gone Before* (visitado el 2 de octubre de 1999) <http://www.fipr.org/publications/consult.html>.

D. La firma digital por medio de los criptosistemas asimétricos

Este esquema asimétrico tiene un beneficio adicional: como el usuario legítimo puede acceder a la información únicamente desencriptándola mediante la clave pública del servicio de archivo, está consciente de que necesariamente ésta fue encriptada con la clave privada del archivo y por ello no sólo sabe que es legítima, sino también conoce que esa información fue necesariamente confeccionada por ese archivo. Por lo tanto, los métodos de encriptado asimétricos no sólo garantizan que el contenido de un documento es inviolable, sino que también certifican la identidad del originante. La certeza respecto al contenido del documento y a la identidad del documento, permite utilizar los criptosistemas asimétricos como firma digital.

La firma digital consiste en encriptar un texto con la clave privada del firmante.[7] El método más idóneo para realizar una transacción, utilizando una firma digital, es el encriptado asimétrico. Para que un documento permanezca secreto, se encripta con la clave pública del destinatario o de quien debe poder acceder a él. Éste, a su vez, desencripta el documento, utilizando su correspondiente clave privada, que sólo él conoce. Los dos métodos se pueden combinar secuencialmente para que el destinatario sólo pueda leer el mensaje y, a la vez, sepa con certeza que el mensaje fue enviado por quien dice haberlo hecho y que no fue alterado de manera alguna en tránsito.[8]

En el ámbito de la documentación digital, el documento encriptado con un sistema asimétrico es el único que se opone a terceros y por ello debe tener fuerza probatoria en un tribunal. Como hemos visto en estos breves ejemplos, el documento sin encriptar es vulnerable en sí mismo, mientras que el documento encriptado de forma simétrica require la divulgación de la clave para ser leído, lo cual exime al originante de toda responsabilidad, dado que un tercero puede haber obtenido y utilizado esa clave en forma fraudulenta. En Estados Unidos, el análisis jurisprudencial indica que la firma digital en base a los criptosistemas asimétricos tiene fuerza probatoria y cumple con la pautas establecidas en el UCC (*Uniform Commercial Code*), mientras que el GAO (*Government*

---

[7] LAWRENCE STREET, *supra* nota 2, en 16.
[8] *Id.*

Accounting Office), de acuerdo a un pedido del NIST, ha dictaminado que las firmas digitales tienen igual validez a las escritas.[9]

E. Autoridades certificadoras

Para que todo este proceso tenga mayor confiabilidad, se ha regulado el mismo creando unos organismos encargados de emitir certificados con el propósito primordial de identificación de las fuentes. Estos organismos se denominan autoridades certificadoras. Estos certificados emitidos electrónicamente, identifican la autoridad certificadora que lo emite, nombra o identifica al subscriptor, consigna la clave pública del subscriptor y está firmado digitalmente por la autoridad certificadora que lo emite.[10] Un ejemplo más práctico de lo qué es un certificado con fines de identificación, es la licencia de conducir. Cuando uno se dirige a cambiar un cheque, en el banco le exigen a uno una identificación. En este caso, la licencia de conducir funciona como un certificado de identidad.

En las transacciones electrónicas, la autoridad certificadora es necesaria para evitar el fraude. Ésta funciona como un sistema de administración de claves que establece reglas claras y concretas sobre el funcionamiento y utilización de las claves, de forma tal que se puedan atribuir válidamente efectos a determinadas situaciones preestablecidas. Dicha autoridad certificadora, previa contestación de la identidad del solicitante, emitirá un certificado que vinculará a dicha persona con su clave pública.

En el ámbito del comercio electrónico, le llamamos certificado a un documento electrónico capaz de identificar la certificadora que lo emite, nombra o identifica al subscriptor, consigna la clave pública del subscriptor y que, además, esté firmado digitalmente por la autoridad certificadora que lo emite. Una vez se acepta el certificado, se entiende que se tiene conocimiento o información sobre su contenido. Cuando esto sucede, el certificado va a un banco de información, que es el sistema desarrollado para recopilar y restablecer certificados y otra

---

[9] Anne Enright Shepherd, *NIST Addresses Practical, Legal Issues to Boost Digital Signature Use* (visitado el 2 de octubre de 1999) <http://www.nist.gov/public_affairs/releases/n94-38.htm>.

[10] Ley de Firmas Digitales de P.R. de 1998, art. 3(6), 3 L.P.R.A. § 1033 (Supl. 1999).

información relevante relacionada con las firmas digitales. Comprender este concepto es de suma importancia, ya que éste determina el valor jurídico de la transacción electrónica cuando se utiliza la firma digital.

F. Ley de Firma Digital del Estado de Utah

El Estado de Utah ostenta, desde mayo de 1995, la primera Ley de Firma Digital en el mundo. La legislación se ha desarrollado a base de un esfuerzo multisectorial, que incluye desde abogados, profesionales de ciencias de computación y especialistas en seguridad de la informática, hasta representantes del Congreso de Utah. Esta Ley de Firma Digital le otorga validez jurídica a los documentos electrónicos o digitales firmados únicamente por medio de criptosistemas asimétricos. No admite ni contempla técnicas alternativas.[11]

Debido a que muchos estados han confrontado problemas en cuanto a la validez jurídica de los documentos electrónicos, muchos de éstos se han unido a la iniciativa de Utah de implementar una legislación que regule este tipo de contratos electrónicos. En octubre de 1995, el estado de California aprobó el *California Digital Signatures Act*. Siguiendo esta misma línea se han unido varios estados. Entre éstos se encuentran: Connecticut, Florida, Georgia, Idaho, Indiana, Illinois, Kentucky, Maryland, Massachusetts, Minnesota, Nebraska, New York, North Carolina, Oklahoma, Oregon, Rhode Island, Texas, Vermont, Virginia, Washington y Wyoming.

G. Normativa de la A.B.A.

La normativa de firma digital ha sido desarrollada por el Comité de Seguridad Informática de la División de Comercio Electrónico y Tecnología Informática, la cual integra la Sección de Ciencias y Tecnología de la A.B.A (American Bar Association). Esta normativa surge de la colaboración de la A.B.A. con el estado de Utah para la confección de su Ley de Firma Digital. La intención es que esta normativa, junto con la Ley de Utah y su reglamentación, sea utilizada por las legislaturas de los restantes cuarenta y nueve estados de la unión

---

[11] Robert J. Stewart , *Utah Digital Signature Program* (visitado el 28 de septiembre de 1999) <http://www.commerce.state.ut.us/digsig/dsmain.htm>.

en la adopción de sus propias leyes de firma digital.[12] Esta inicativa provocó que el presidente Clinton firmara recientemente el *Electronic Signature in Global and National Commerce Act,* que otorga valor jurídico a la firma digital. La misma entrara en vigor el 1 de octubre del 2001.

H. Usos actuales del criptosistema asimétrico

Estas garantías de remitente, contenido y destinatario sientan las bases del comercio electrónico para facturación y pago electrónico entre grandes empresas y sus bancos y para hacer compras en la Internet. El que dispone de acceso a la Internet puede visitar el primer banco que opera exclusivamente en el Internet, el *Security First Network Bank*. Este banco no contempla atender al público en la forma tradicional, sino únicamente por correo electrónico o de papel y por medio del *Web*, naturalmente. El *Security First Network Bank* ofrece cuentas corrientes con chequeras, tarjetas de crédito, tarjetas de cajeros automáticos, préstamos personales, hipotecas y una línea completa de servicios de corretaje. ¿Qué tan serio y seguro es este banco? *El Security First Network Bank* cuenta con una autorización para operar, expedida por el Federal Reserve Bank, además de $100,000.00 de garantía por cada cuenta de cliente, otorgada por el *Federal Deposit Insurance Corporation*, la agencia que asegura los depósitos bancarios en los Estados Unidos. Dada su eficiente estructura de costos, el *Security First Network Bank* puede ofrecer sus servicios gratis y sólo requiere de $100 como depósito inicial para abrir una cuenta. Tampoco es necesario contar con un programa o *software* especial, sino que basta con el *Web browser* para operar con este banco.[13] El *Security First Network Bank* es un ejemplo del comercio electrónico que es posible mediante la firma digital por medio de criptosistemas asimétricos. Además de esto, en los Estados Unidos los sistemas interbancarios de transferencia de fondos (*Fed-Wire y Chips*, que mueven billones de dólares a diario) y el sistema seguro de comunicaciones entre bancos internacionales (*SWIFT*) ya utilizan estas técnicas hace décadas.[14]

---

[12]American Bar Association, Section of Science and Technology, Information Security Committee, DIGITAL SIGNATURE GUIDELINES (1996).

[13] Security First Network Bank, *The World's First Internet Bank* (visitado el 24 de septiembre de 1999) <http://www.sfnb.com/infodesk/about.html>.

[14]Amelia H. Boss, *The Emerging Law of International Electronic Commerce*, 6 TEMP. INT'L & COMP. L.J. 293 (1992).

I. Ley de Firmas Digitales de Puerto Rico

El 7 de agosto de 1998, la Asamblea Legislativa aprobó la Ley 188 de Firmas Digitales de Puerto Rico. El propósito de ésta es reconocer a la rúbrica digital, que se realiza a través de claves de algoritmo, el mismo efecto legal que se reconoce en nuestro ordenamiento a la firma de puño y letra.[15] Junto con esto, se pretende: autorizar y reglamentar el uso de firmas digitales, facultar al Departamento de Estado para conceder licencias a las autoridades certificadoras, establecer los requisitos y salvaguardas necesarios para garantizar la confidencialidad de las firmas, además de establecer penalidades a los que violen las disposiciones de esta Ley.[16]

La Ley de Firmas Digitales contempla dos factores claves en el funcionamiento de este proceso. Uno es el uso de criptosistemas asimétricos y el otro, es el papel regulador de las autoridades certificadoras. Según la Ley Firmas Digitales, mediante el uso de un criptosistema asimétrico, se establecen dos claves:

1) la clave privada, que es la que se utiliza para crear la firma digital;
2) y la clave pública, que es utilizada para verificar la firma digital.

Este proceso es regulado por una autoridad certificadora. El Departamento de Estado funciona como una autoridad certificadora y es, además, quien concede las licencias a estas entidades. Es de suma importancia que la autoridad certificadora posea la licencia expedida por el Departamento de Estado. La licencia otorgada por el Departamento de Estado será el factor clave que va a determinar el límite máximo de responsabilidad por posibles daños.[17] Las operaciones de cada una de las autoridades certificadoras licenciadas serán auditadas por un contador público autorizado, un perito en seguridad de computadoras o un profesional acreditado en seguridad de computadoras, por lo menos una vez al año, para evaluar el cumplimiento de las disposiciones de esta Ley.

a. Emisión del certificado

[15] Ley de Firmas Digitales de P.R. de 1998, art. 1, 3 L.P.R.A. § 1031 (Supl. 1999).
[16] Ley de Firmas Digitales de P.R. de 1998, art. 7, 3 L.P.R.A. § 1033f (Supl. 1999).
[17] Ley de Firmas Digitales de P.R. de 1998, art. 17, 3 L.P.R.A. § 1033i (Supl. 1999).

La autoridad certificadora emitirá un certificado a un subscriptor si éste cumple con presentar la correspondiente solicitud y si la autoridad certificadora verifica lo siguiente:

(a) que el subscriptor 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 subscriptor es el tenedor legal de la clave privada que corresponde a la clave pública que se designa en el certificado;

(e) que el subscriptor es tenedor de una clave privada capaz de producir una firma digital;

(f) que la clave pública indicada en el certificado puede ser utilizada para verificar una firma digital con la clave privada que tiene el subscriptor.[18]

Si el subscriptor acepta el certificado emitido, la autoridad certificadora publicará una copia firmada del certificado en un banco de información reconocido, determinado por ambos, a menos que se provea otra cosa por contrato. Si el subscriptor no acepta el certificado, la autoridad certificadora licenciada no lo publicará o cancelará su publicación si el mismo ha sido publicado. El Departamento ordenará a la autoridad certificadora que suspenda o revoque un certificado, previa notificación y vista a la autoridad certificadora y al subscriptor, cuando determine que el certificado no cumple con los requisitos establecidos por las disposiciones de la Ley de Firmas Digitales y que el incumplimiento representa un riesgo significativo para las personas que se valen del certificado.[19]

b. Garantías y obligaciones de la autoridad certificadora

La autoridad certificadora licenciada, al emitir un certificado, garantiza al subscriptor que el mismo no contiene información falsa, que cumple con los requisitos que establece esta Ley y que ha actuado dentro de la autoridad que le confiere la licencia que se le ha expedido. La

---

[18] Ley de Firmas Digitales de P.R. de 1998, art. 10, 3 L.P.R.A. § 1033e (Supl. 1999).
[19] *Id.*

autoridad certificadora licenciada no podrá renunciar o limitar las garantías.[20] Ésta tiene lo que se denomina un límite máximo de responsabilidad, que es el monto de la cantidad fijada en un certificado que responde por los daños y perjuicios ocasionados. Al establecer un límite máximo de responsabilidad en un certificado, la autoridad certificadora licenciada y el subscriptor advierten a las personas que se valen del mismo que el riesgo no está cubierto por una cantidad mayor al límite máximo fijado.[21] Este aspecto es muy controversial, debido a que limita la garantía de seguridad sobre el valor de la transacción a un límite establecido por la autoridad certificadora. Esto crea un obstáculo en el tipo de negocios que se podrían efectuar a través de este sistema. Crea una incertidumbre en cuanto a la seguridad de la transacción y cómo va a responder la autoridad certificadora en caso de que se violenten de algún modo estos parámetros.

II. Análisis

A. Transición del notario puertorriqueño

Una vez visto este panorama, tenemos que analizar qué impacto tendrá este tipo de legislación en la profesión jurídica. El factor clave en este tipo de transacciones es la certificación. Esto debido a que de ésta depende el valor jurídico de la transacción. La necesidad de regular este aspecto crea un nuevo campo en el Derecho. Es de aquí que surge la necesidad de un notario capacitado en seguridad dentro del campo de la informática. La autoridad certificadora juega un rol clave en el marco de las transmisiones electrónicas de mensajes. Por esta razón, se debe establecer un sistema de reglas de conducta destinadas a garantizar que sus funciones puedan cumplirse correctamente. Resulta interesante notar que la doctrina establece exigencias que son comparables a los principios del notariado latino, pero con ciertas diferencias. Así mismo, es interesante la singular coincidencia en la definición de la autoridad certificadora (en tanto tercero de confianza) y la definición clásica del notario. La declaración acerca *del notario y su función*, adoptada por unanimidad en la Conferencia de Notariados de la Unión Europea realizada en Madrid el 23 de marzo de 1990, brinda la siguiente

[20] Ley de Firmas Digitales de P.R. de 1998, art. 7, 3 L.P.R.A. § 1033f (Supl. 1999).
[21] *Id.*

definición: "el notario es un oficial público que tiene una delegación de la autoridad del estado para dotar a los documentos que redacta y de los cuales él es el autor, el carácter de autenticidad que confiere a dichos documentos, cuya conservación asegura la fuerza probatoria y la fuerza ejecutiva".[22]

En primer lugar, debemos clarificar que los estados que han deliberado acerca de las transacciones jurídicas electrónicas entienden que la certificación de claves constituye una actividad que puede ser ofrecida comercialmente, pero que ello no excluye la existencia de otras organizaciones que funcionen en forma paralela. De hecho, la legislación de firmas digitales implementada en Puerto Rico establece los requisitos para obtener la licencia del Departamento de Estado como autoridad certificadora y de forma alguna excluye a la clase notarial.[23] Por el

---

[22] Unión Internacional del Notariado Latino, Comisión de Informática y Seguridad Jurídica, *El notario y las transacciones jurídicas electrónicas* (visitado el 22 de septiembre de 1999) <http.//www.colegio- escribanos.org.ar/traduccion.htm>.

[23] Ley de Firmas Digitales de P.R. de 1998, art. 5, 3 L.P.R.A. § 1032 (Supl. 1999). 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 subscriptor 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 apruebe 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;

contrario, la Ley Notarial de Puerto Rico del 2 de julio de 1987, establece unas limitaciones en cuanto al tipo de firma y a la forma en la cual se tienen que identificar los otorgantes en una transacción. El artículo 16 y 17 de la Ley Notarial establecen lo siguiente:

> Art 16. Los otorgantes y los testigos firmarán la escritura y además estamparán las letras iniciales de su nombre y apellido o apellidos al margen de cada una de las hojas del instrumento, las cuales rubricará y sellará el notario.
>
> Art. 17. Serán medios supletorios de identificación, en defecto del conocimiento personal del notario:
> (a) La afirmación de una persona que conozca al otorgante y sea conocida por el notario, siendo aquélla responsable de la identificación y el notario de la identidad del testigo.
> (b) La identificación de una de las partes contratantes por la otra, siempre que de esta última se de fe de conocimiento del notario.
> (c) La identificación por documento de identidad con retrato y firma, expedido por las autoridades públicas competentes de Estado Libre Asociado de Puerto Rico, de los Estados Unidos, o de uno de los estados de la Unión, cuyo objeto sea identificar a las personas o por pasaporte debidamente expedido por autoridad extranjera.
>
> Los testigos de conocimiento serán responsables de la identificación de los otorgantes, igualmente lo será el otorgante que testifique sobre la identidad de otros otorgantes no conocidos por el notario y el notario lo será del conocimiento de tales testigos.

Como se puede apreciar, la Ley Notarial no armoniza con los elementos de la nueva Ley de Firmas Digitales. Esto se debe a que la tradición notarial en Estados Unidos es una sumamente flexible. En Puerto Rico, la tradición notarial se deriva del Derecho Civil y es muy restrictiva. Esta situación crea un gran problema, debido a que en Puerto Rico los únicos autorizados a dar fe pública son los notarios, no se contempla ni se autoriza la figura de una autoridad certificadora para que ésta dé fe pública. Es por esta razón que el carácter de la actividad notarial debe llevarse a un escrutinio legislativo para estudiar y analizar si la misma debe ser mantenida como se encuentra en el presente, sujeta a ciertas exigencias o debe enmendarse para que los notarios intervengan paralelamente con comerciantes u otros prestatarios de servicio de

---

(h) cumplir con todos los demás requisitos establecidos mediante reglamento por el Departamento.

certificación que ejerzan su actividad en el marco de una profesión liberal.

B. El notario cibernético como un oficial de seguridad

La American Bar Association ha destacado la importancia de la participación del notario, entre otras cosas, en el proceso de identificación y recepción de las solicitudes de certificados. Como un oficial de seguridad en el comercio electrónico que combina experiencia técnica y legal, el notario cibernético tendrá competencia para intervenir en transacciones dentro de una escala muy amplia, que requerirá distintos tipos de seguridad, según la clase de transacción de que se trate.[24] La práctica del notario cibernético, dentro del marco de una infraestructura de clave pública, comprenderá intervenciones que abarcarán desde la verificación de los datos de una persona (a efectos de la registración de una clave pública y obtención de un certificado) hasta la certificación de la identidad y capacidad de una persona (con el objeto de realizar una transacción) y a la autenticación de que una transacción cumple los requisitos legales y formales.

De esta forma, el notario cibernético tendrá dos funciones en el comercio electrónico basado en una estructura de clave pública. La primera de ellas será la de realizar una investigación de los usuarios que deseen registrar sus claves públicas para su utilización en el comercio electrónico. Dado que la política y procedimientos para la registración serán establecidos por la autoridad certificadora, los pasos a seguir por el notario cibernético para registrar al usuario variarán de acuerdo al grado de certificación que dicha autoridad desee proveer. La segunda función tiene que ver con el valor de la certificación. Para una certificación de bajo valor, se podrá requerir al notario cibernético para establecer la identidad del usuario y asignarla a la llave pública.

En el caso de certificaciones de alto valor, el notario cibernético puede ser requerido para realizar una exhaustiva investigación sobre el usuario, incluyendo su historia crediticia, criminal, etc., antes de que la clave pública sea emitida y certificada.[25] Al ser un campo que conlleva un

---

[24] Theodore S. Barassi, *Electronic Commerce* (visitado el 25 de septiembre de 1999) <http://www.abanet.org/scitech/ec/cn/home.html>.

[25] Joseph Kornowski, *The Specter of the CyberNotary: Science Fiction or New Legal Specialty?* (visitado el 16 de septiembre de 1999)

conocimiento mayor del Derecho, esto trae como consecuencia que el típico notario anglosajón ya no esté capacitado para llevar a cabo este tipo de trabajo. Esto, a su vez, repercute en una transición del notario anglosajón al notario de tradición civilista.

C. Desarrollo de un campo especializado

El desarrollo del notario cibernético abre una nueva rama de especialización en el campo del Derecho. El notario cibernético tendrá un amplio conocimiento en el campo de la seguridad de información electrónica, el cual, hasta hace poco, era desconocido para la mayoría de los notarios. Para poder comprender cómo se ha ido delimitando este nuevo campo, veamos el desarrollo de ARKANVS, una de las dos primeras autoridades certificadoras licenciadas por el estado de Utah. Esta empresa ha incorporado la figura del *CryptoNotary* como autoridad de registración. *CryptoNotary* ™ es una marca registrada por *ARCANVS, Inc*. El proceso *CryptoNotary* ™ se encuentra patentado por *ARKANVS*. Un *CryptoNotary* ™ es un notario público calificado que utiliza el *ARCANVS CryptoNotary* ™ *software* para

1) verificar la identidad del suscriptor,
2) dejar constancia de los documentos de identificación,
3) firmar digitalmente la solicitud de certificado del usuario, y
4) remitir la solicitud a *ARKANVS* para la verificación final y emisión del certificado.[26]

El proceso *Cryptonotary* ™ constituye un estándar para la verificación de la identidad del suscriptor y todas las funciones notariales digitales. De acuerdo a las regulaciones del gobierno federal, un sistema que permita la utilización de notarios para estos fines sólo podría ser implementado si la legislación estatal o federal reconociera la firma digital del notario público como equivalente a la firma física ológráfica y la certificación digital y la correspondiente firma digital sean reconocidas sin necesidad de que sean acompañadas por un sello notarial de tipo físico. De acuerdo a estos criterios, podemos llegar a la conclusión de que en Puerto Rico se puede implementar una práctica notarial a base del registro y certificación de documentos electrónicos, mediante el uso de firmas digitales. Siempre

---

<http://www.lacba.org/lalawyer/tech/notary.html>.

[26] Gordon W. Romney, *The CryptoNotary* (visitado el 25 de septiembre de 1999) <http://www.cryptonotary.com/info.html>.

y cuando se armonice la Ley notarial y su reglamento con la nueva Ley de Firmas Digitales.

D. Surge una nueva figura en el *Common Law*

Según lo dispuesto por la American Bar Association, el notario cibernético es un abogado facultado para ejercer en el territorio de los Estados Unidos y calificado para actuar como *CyberNotary* de acuerdo a las reglas desarrolladas por la ABA.[27] El problema que esto ocasiona es que la función del *CyberNotary* se asemeja a la de un notario de tradición civilista. A todo esto, debemos sumar que las funciones del *CyberNotary* y el notario cibernético de tradición civilista van dirigidas a las transacciones internacionales por medio de las computadoras. Esto trae, como consecuencia, un punto convergente entre el notario del *common law* y el de tradición civilista.

El sector privado ofrece cada día nuevas soluciones al problema de la seguridad. De más está decir que, en muchos casos, los servicios que las soluciones informáticas brindan el mismo nombre que ciertas garantías que sólo brinda el sistema de notariado de tradición civilista. Paralelamente a la estructura legal tradicional antes referida, fue desarrollándose una infraestructura de seguridad en el ámbito informático. En tanto los dos mundos vivieron en forma independiente, no hubo conflictos. La denominada *network security* ofrecía soluciones para las interrogantes planteadas en el mundo de la informática (identidad de las personas, confidencialidad e inalterabilidad de los mensajes), mientras los sistemas o estructuras legales de los distintos países hacían otro tanto en el mundo tangible.

La convergencia y la revolución digital están haciendo de ambos mundos uno solo y la compleja red de seguridad informática, que hasta ahora se mantenía circunscrita al ámbito de las soluciones informáticas, está trabajando frente al desafío que el nuevo medio implica para la comunidad jurídica. Sin embargo, la adecuación de las soluciones del mundo digital al mundo de papel no resulta ser tan simple como parecería en un principio. En primer lugar, no existe uniformidad terminológica. Muchas veces coincide la denominación de los servicios que los sistemas

---

[27] Theodore S. Barassi, *The CyberNotary: Public Key Registration and Certification Services for International Electronic Commerce* (visitado el 2 de octubre de 1999) <http://www.irnex.com/uscib/news/foicybnt.htm>.

(mundo digital - mundo de papel) ofrecen (*trust, security, non-repudiation, signature, integrity*), pero su significado y la forma de satisfacerlos, lógicamente, son totalmente distintos.

Mientras todo esto sucede, el notario anglosajón, que no tiene que ser abogado, sigue desempeñando sus funciones en el mundo de papel. Esto significa que la aparición del *CyberNotary* no ha relevado de su trabajo al típico notario anglosajón. El *CyberNotary* ha surgido como una nueva figura dentro del *common law* con unas funciones determinadas dentro del campo de la informática. Según se vaya regulando de forma uniforme el uso de la firma digital, entendemos que el *CyberNotary* pasará a ser una figura central dentro del *common law*.

Por otro lado, las soluciones del mundo de papel varían según el sistema jurídico imperante en cada país. Ello conduce a que la transición del mundo de papel al mundo digital en los países donde rige el *common law* no pueda ser encarada de la misma forma ni con las mismas estructuras que en los países donde rige el Derecho Civil. Este problema exige un estudio de Derecho Comparado para lidiar con las diferencias entre ambos sistemas. La figura del notario cibernético puertorriqueño tiene el mayor potencial para lidiar con este problema de divergencia. Esto debido a su formación legal tanto en el Derecho Civil como en el *common law*. Es por eso que la Ley de Firmas Digitales de Puerto Rico le ha abierto las puertas al notario puertorriqueño para que desempeñe un papel muy importante en el comercio internacional a través de los medios electrónicos.

III. Recomendaciones

A. Que se armonice la Ley notarial y el Reglamento notarial con la Ley de firmas digitales

Esta situación es de suma trascedencia, de llevarse a cabo dicha propuesta, el notario puertorriqueño estaría abriéndose las puertas a una infinidad de oportunidades en el campo del comercio electrónico, que está en constante crecimiento. La legislatura tiene que decidir si va enmendar la Ley Notarial para dos propósitos: (1) armonizar los procedimientos y los conceptos de la Ley Notarial con la Ley de Firmas Digitales (2) y para permitir que autoridades certificadoras que no son parte de la clase notarial puedan dar fe pública o si, por el contrario, le

exige a estas autoridades certificadoras que utilicen notarios para tales fines. Nosotros nos inclinamos a pensar que armonizar los procedimientos y conceptos de ambas leyes es vital para poder implementar la Ley de Firmas Digitales. En cuanto al segundo punto, entendemos que es más conveniente que se le exija a estas autoridades certificadoras que un notario sea el que de fe pública para así brindar mayor confianza a las transacciones.

B. Desarrollar la infraestructura de las agencias gubernamentales

Dicha legislación requiere que las dependencias gubernamentales realicen sus transacciones por sistemas electrónicos, minimizando el uso del papel y acelerando la calidad de sus servicios. Debido a que uno de los objetivos principales de la Ley es agilizar la efectividad y eficiencia de los procesos en dichas agencias.

C. Preparación de los notarios en materia de informática, firma digital y encriptado

Es de suma importancia que se implemente un programa de adiestramiento, en cuanto a los conceptos básicos de informática. Se debe educar a los notarios en la utilización práctica de los componentes necesarios como la implementación de computadoras, impresoras, *smart cards*, lector de *smart cards*, procesador de texto, redes, comunicación a distancia, firma digital y encriptado.

D. Creación de una infraestructura notarial para el registro y la certificación de firmas digitales

Ya que la Ley de Firmas Digitales de Puerto Rico no excluye a la clase notarial de ser una autoridad certificadora o registradora,[28] se debe establecer una infraestructura para que la clase notarial puertorriqueña comience a trabajar como una autoridad certificadora o registradora. Consideramos viable la puesta en marcha de una infraestructura que permita a los notarios ofrecer servicios de certificación en el marco de las actividades autorizadas por ley. En el caso de que surgiese alguna

[28] Unión Internacional del Notariado Latino, *supra* nota 22.

controversia, en la cual las disposiciones de carácter general no resulten aplicables en forma apropiada, las organizaciones profesionales deberán emitir recomendaciones para la prestación práctica de servicios de certificación.

E. Colaboracíón de las organizaciones profesionales

En cuanto a este aspecto, consideramos que las organizaciones profesionales deben proveer una comunicación electrónica segura y efectiva. Se debe adoptar la comunicación por correo electrónico, como un medio eficiente de comunicación entre la profesión jurídica. Además, es necesario crear redes de comunicación notariales a través de *intranets*. Por último, es preciso establecer fuentes propias de información electrónica, como, por ejemplo, registros de testamentos, información relativa a bienes inmuebles, información científica, etc.

F. Elaborar un reglamento que regule el funcionamiento y la seguridad de la información en las autoridades certificadoras

1. Protección de los Datos

Se debe establecer una norma general que establezca que no podrán realizarse transferencias temporales, ni definitivas, de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento, a países que no gocen de un nivel de protección equiparable al que preste la Ley de Firmas Digitales de Puerto Rico. Las leyes de protección de datos no deben suponer un freno a la transferencia de información, sino sólo la seguridad de que lo que se transfiere es lo correcto. El derecho a la intimidad y el reclamo a recibir información están en colisión permanente y ello no es nuevo, sino que ha venido sucediendo a través de los tiempos. Lo que debe hacerse es buscar el equilibrio necesario entre ambos puntos.

2. Seguridad en la autoridad certificadora

En la autoridad certificadora la protección no ha de basarse sólo en dispositivos y medios físicos, sino en formación e información adecuada al personal, empezando por el directivo para que, en cascada, afecte

todos los niveles de la pirámide organizativa. La existencia de funciones específicas, cuando el entorno lo justifica, contribuye a incrementar la seguridad, entre ellas la de administración de la seguridad y auditoría de sistemas de información interna. Ambas funciones han de ser independientes y nunca una misma persona podrá realizar las dos ni podrá existir dependencia jerárquica de una función respecto a otra. En cuanto a la administración de seguridad, pueden existir, además, coordinadores en las diferentes áreas funcionales y geográficas de cada entidad, especialmente si la dispersión o la complejidad organizativa o el volumen de la entidad así lo demandan. Deben existir tres niveles de protección: el control interno, basado en objetivos de control y llevado a cabo por los supervisores a distinto nivel, y la auditoría de información interna, objetiva e independiente y con una preparación adecuada, como control del control. La auditoría de sistemas de información externa es otro método de seguridad que debe implementarse, como un nivel de protección adicional, a la que obliga la Ley de Firmas Digitales de Puerto Rico. Los informes de auditores, internos o externos, han de señalar las posibles deficiencias e indicar, en su caso, las recomendaciones correspondientes. Si no existe una idea clara de cuáles son los riesgos, debe hacerse una evaluación de dichos riesgos por personas objetivas e independientes y técnicamente preparadas.

IV. Conclusión

A base de un análisis práctico, entendemos que la Ley de Firmas Digitales de Puerto Rico ha abierto una brecha de gran significado para el abogado que labora en el campo del Derecho Notarial. Para que esto sea una realidad es necesario armonizar los conceptos y procedimientos de la Ley Notarial con la Ley de Firmas Digitales. En primer lugar, debemos aclarar que la Ley de Firmas Digitales de Puerto Rico expone que la certificación de claves constituye una actividad que puede ser ofrecida comercialmente, pero que ello no excluye la existencia de otras organizaciones que funcionen en paralelo.[29] Así como sucede en el área tradicional de actividad del notario, donde el notario, en su calidad de ofrecer un oficio público, entre otros, presta su asistencia y consejo en concurrencia con otras profesiones. El carácter de la actividad notarial,

[29] *Id.*

sujeta a ciertas exigencias, será mantenido, aun en el caso que intervengan paralelamente con comerciantes u otros prestatarios de servicio de certificación que ejerzan su actividad en el marco de una profesión liberal. El conflicto que representa esta situación es que el elemento de la fe pública sólo le es otorgado al notario por el Estado. Entendemos que es más conveniente que se le exija a estas autoridades certificadoras que un notario sea el que dé fe pública para así brindar mayor confianza a las transacciones. Que éstas estén obligadas a emplear notarios para sus funciones.

Otro elemento clave en la transición del notario tradicional al notario cibernético es la adquisición e implementación de la tecnología adecuada para llevar a cabo transacciones electrónicas. Así como el notario necesita hacer uso de los productos disponibles en el mercado relacionados a su equipamiento técnico (material informático, sellos, productos para escribir), en el ámbito de las transacciones electrónicas la utilización de los componentes necesarios y cooperación de prestadores de servicios técnicos le permitirá ofrecer diversos servicios notariales que implicarán meramente el transporte de sus funciones tradicionales al mundo electrónico, sin que se vea afectada su imagen. En este marco, el notario, en su carácter de prestatario de servicios jurídicos, ofrece, además de una gran cualificación jurídica, un valor agregado, al tiempo que utiliza las facilidades técnicas disponibles que tendrá que manejar para llevar a cabo su función en las transacciones electrónicas.

En cuanto a la función individual del notario en la prestación de servicios de certificación, se puede visualizar un desempeño en calidad de instancia de registro para las autoridades certificadoras, actividades que garanticen la seguridad jurídica de los interesados (consultoría y asesoramiento con relación a las transacciones que se negocien y concluyan en forma electrónica) y otras que protejan la documentación y la prueba en el ámbito de las transacciones jurídicas electrónicas (confirmación del envío y de la recepción, archivo electrónico de documentos, etc.)

A base de todo este análisis, concluimos que el notario cibernético puertorriqueño va a ejercer su función pública en el marco de una profesión liberal, legal y tecnológica. Además, deberá responder con el nivel jurídico esperado tanto en las transacciones jurídicas en documentos de papel como en las que se realicen por vía electrónica. En cuanto a las autoridades certificadoras de clave pública, se vislumbra una actuación

conjunta entre los nuevos actores y los notarios tradicionales. La identificación del solicitante de un certificado de clave pública constituye una de las funciones que el notario puede brindar dentro de una infraestructura de firma digital, complementando la actividad de estos nuevos actores. Todos estos cambios surgen como consecuencia de la alta demanda de medidas de seguridad en el comercio electrónico. Es por esta razón que ha surgido la necesidad de regular esto mediante una legislación que imponga unas pautas, dándole confiabilidad a la transacción electrónica mediante la firma digital, ya que ésta se ha convertido en un elemento clave de la economía mundial. La Ley de Firmas Digitales nos abre una puerta al comercio internacional , pero hay que enmendarla para así evitar un conflicto con las disposiciones de la Ley Notarial, la cual representa la tradición notarial existente en Puerto Rico.