



IUS. Revista del Instituto de Ciencias Jurídicas
de Puebla A.C.

ISSN: 1870-2147

revista.ius@hotmail.com

Instituto de Ciencias Jurídicas de Puebla A. C.
México

Formentín Zayas, Yanixet Milagro

La firma electrónica, su recepción legal. Especial referencia a la ausencia legislativa en Cuba
IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., vol. VII, núm. 31, enero-junio, 2013,
pp. 104-120

Instituto de Ciencias Jurídicas de Puebla A. C.
Puebla, México

Disponible en: <http://www.redalyc.org/articulo.oa?id=293227561007>

- Cómo citar el artículo
- Número completo
- Más información del artículo
- Página de la revista en redalyc.org

redalyc.org

Sistema de Información Científica
Red de Revistas Científicas de América Latina, el Caribe, España y Portugal
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

La firma electrónica, su recepción legal. Especial referencia a la ausencia legislativa en Cuba*

*The electronic signature, its legal reception.
Special reference to legislative void in Cuba*

Yanixet Milagro Formentín Zayas**

RESUMEN

La seguridad de las transacciones electrónicas resulta ser uno de los aspectos controversiales en la era digital. A partir de la aparición del comercio electrónico en la contratación internacional cubana, los intereses en cuanto a resguardar su autenticidad y seguridad han sido el talón de Aquiles de los profesionales del derecho y del comercio. La respuesta internacional estuvo en la promulgación de la Ley Modelo de la UNCITRAL sobre Comercio Electrónico en 1996, y en 2001 la Ley Modelo de la UNCITRAL sobre Firma Electrónica. Los Estados, en respuesta, emitieron diferentes disposiciones normativas sobre la temática, aparejadas a tales avances. La solución legislativa cubana aún está por llegar. Constituye ésta la certeza jurídica de la firma electrónica en Cuba con condiciones diferentes a las existentes en otros países.

PALABRAS CLAVE: Contratación electrónica, firma electrónica, ley modelo sobre firma electrónica, seguridad de la contratación electrónica.

ABSTRACT

The security of electronic transactions is one of the most controversial aspects in the digital age. From the appearance of the electronic commerce in Cuban Int'l hiring, the interests in safeguarding authenticity and safety has been the Achilles' heel of legal and trade professionals. The Int'l answer was the promulgation of the UNCITRAL Model Law on Electronic Commerce in 1996 and the UNCITRAL Model Law on Electronic Signatures in 2001. The states issued different normative provisions on the topic and today, we can speak about a legal framework existing in many countries. The Cuban legislative solution is still to come. It is only a project due to mistakes of fate. This is the legal certainty of the electronic signature in Cuba, under conditions different from those existing in other countries.

KEY WORDS: Electronic hiring, electronic signature, model law on electronic signature, safety of the electronic hiring.

* Recibido: 1 de octubre de 2012. Aceptado: 13 de noviembre de 2012.

** Profesora de Derecho mercantil en la Facultad de Derecho de la Universidad de Camagüey, Cuba.
(yanicet.formentin@reduc.edu.cu).

Sumario

1. La firma electrónica. Aspectos doctrinales
2. Labor unificadora de la firma electrónica en el marco de las Naciones Unidas y estatal
3. La futura ley cubana
4. A manera de conclusión

1. La firma electrónica. Aspectos doctrinales

La noción de firma encierra usualmente la imagen de que debe ser manuscrita, lo que presume la máxima garantía de la autoría. Con la irrupción de las tecnologías es obvio que el requisito de firma manuscrita no puede cumplirse en los documentos electrónicos,¹ por lo que se conciben nuevas modalidades de comprobación de identidad, de consentimiento, de autenticidad y de integridad de los documentos. De ahí que exista cierta tendencia en el ámbito del comercio internacional a suprimir, o al menos descubrir sustitutos de la firma,² que logren el mismo efecto legal. Entre estos medios similares fiables se encuentran las firmas “electrónicas” o “digitales”.³

La firma electrónica o digital es un conjunto de datos electrónicos que identifican a una persona en concreto. Suelen unirse al documento que se envía por medio telemático, como si de la firma tradicional y manuscrita se tratara, de esta forma el receptor del mensaje está seguro de quién ha sido el emisor, así como la seguridad de que el mensaje no ha sido alterado o modificado.

La firma electrónica puede utilizarse en el sector privado, para contratación privada por vía electrónica, entre empresa y consumidor (por ejemplo, la compra de un libro o un compacto por Internet) y entre empresas (por ejemplo, realizar un pedido a un distribuidor) o incluso entre los mismos consumidores finales

¹ Las reproducciones electrónicas de la firma, o cualquier otro signo aparente, presentan el problema antes aludido de la perfecta modificabilidad de los soportes electrónicos: la firma podría ser transferida a otro documento, y el documento firmado ser alterado de modo indetectable. Véase SIMÓ SEVILLA, DIEGO. “Las nuevas modalidades de presentación del consentimiento: la función notarial”, en *Notariado y contratación electrónica*, Colegios Notariales de España, Madrid, 2000, p. 413.

² Por ejemplo, las Reglas de Hamburgo (Convenio de las Naciones Unidas sobre el Transporte Marítimo de Mercancías), en el artículo 14.3, permiten que la firma sea manuscrita, impresa en facsimile, perforada, sellada, en símbolos o hecha por cualquier otro medio mecánico o electrónico.

³ A los efectos de la presente investigación, la firma electrónica trata de dar solución a los problemas de fraude y falta de autenticidad del documento; no obstante, se reconoce que existen otras técnicas que contribuirían a tal garantía, tal es el caso del reconocimiento electrónico de datos biométricos (huellas digitales, vasos sanguíneos de la retina, la propia firma del interesado realizada con un lápiz electrónico y reconocida por el ordenador, etcétera). Pero este tipo de medios presentan ciertos problemas, que sólo funcionan a modo de clave de acceso a la máquina o a la red en la que se trasmite el documento, pero no se unen al documento mismo, y además crean problemas, como negativas erróneas de acceso por no reconocer el sistema al propio titular de la clave.

(por ejemplo, venta de una raqueta de segunda mano, una colección de monedas, entre otros).

También sirve para realizar actuaciones con y entre la administración, es decir, sirve tanto para las relaciones entre los propios entes públicos que la forman, como para las relaciones del ciudadano con la administración (por ejemplo, algo tan simple como la renovación del DNI, la solicitud de prestaciones a la seguridad social o incluso la presentación de la declaración de la renta por Internet con el conocido programa "Padre").

Su umbral se desarrolló a partir de una oferta tecnológica para acercar la operatoria social usual de la firma manuscrita al marco de lo que se llamó el trabajo en redes, fue introducida por DIFFIE y HELLMAN.⁴ La evolución de este concepto es notable, y no sólo se concibe la firma electrónica desde un ángulo numérico o matemático, sino también jurídico. *Grosso modo*, la definición de lo que se entiende por firma electrónica es vital a fin de su mejor comprensión desde ambos puntos de vistas.

El debate en cuanto al concepto de firma electrónica es uno de los que hoy centra el estudio del derecho informático, como fenómeno técnico-jurídico que brinda seguridad, autenticidad y confianza a las relaciones jurídicas de los empresarios en la red. El paulatino interés por estudiar la firma electrónica y sus efectos en las diferentes legislaciones ha hecho que su definición sea difícil de consolidar; sin embargo, la mayoría de las acepciones que a continuación se analizan guardan cierta analogía porque contienen similares elementos.

En relación con el vocablo, las nociones se manifiestan mayoritariamente desde el punto de vista técnico y otras en un sentido jurídico. En el primer matiz, las definiciones más acertadas se encaminan a considerar la firma electrónica como "una señal digital representada por una cadena de bits..., un término teórico que indica tanto un texto como las huellas digitales exportadas al pie de un escrito, y así mismo, al código o clave de acceso a un sistema informático, en el cual el agente titular exterioriza su voluntad".⁵ Otra parte de la ciencia admite

⁴ DIFFIE y HELLMAN crearon un método denominado "acuerdo de distribución de claves", que permitió que dos entidades acuerden una clave asimétrica sin necesidad de comunicación previa. El algoritmo propuesto por estos científicos se basó en emplear una función unidireccional con trampa, donde a cada valor de x le corresponde una y , y viceversa, por lo que dado un valor de y es fácil calcular x , y se hace difícil para aquellos que no tienen conocimiento de esta información. La función empleada por DIFFIE y HELLMAN es la exponencial discreta, cuya inversa, el algoritmo discreto es difícil de calcular. En 1976 estos dos investigadores norteamericanos descubren lo que se denomina la criptografía de clave pública y, como consecuencia de esta, la firma digital. En 1977, RON RIVEST, ADI SHAMIR, y LEN ADLEMAN, del Instituto Tecnológico de Massachusetts (MIT), proponen el hasta hoy más usado método de firma digital, denominado RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública. En la actualidad, RSA es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

⁵ BAUZÁ, MARCELO. "Firma electrónica y entidades certificadoras", en *Jornadas de Comercio Electrónico*, Ed. Instituto de Derecho Comercial, Madrid, 2002, p. 173; PESO NAVARRO, EMILIO. "Resolución de conflictos en el intercambio electrónico

que es “un medio que posee la persona para probar quién envió el mensaje y cuál es su contenido”.⁶

Merece atención apuntar las ideas aportadas por MUÑOZ ROLDÁN, quien cita a BELDA CASANOVA, al manifestar que la firma electrónica es “el procedimiento en virtud del cual se puede imputar a una persona, el contenido de un mensaje que viaja por la red”.⁷ Se debe resaltar, en el concepto, la correlación de los dos matices, de un lado como algo positivo, la imputación del contenido a quien realiza el mensaje y lo envía y no es así a quien lo recibe, por lo menos hasta que no lo confirme, y del otro, valido criticar el considerarla un procedimiento en sí mismo no un requisito del mensaje.

Al margen del tópico técnico, emergen otras cuestiones de carácter jurídico, relacionadas con la concepción que sobre la firma manuscrita existe. Las primeras posturas cardinales hicieron aportes en la materia; se citan como ejemplo aquellos que revelan la firma electrónica como un atributo del mensaje de datos que significa al autor y la inalterabilidad del contenido del documento, luego de ser confirmado,⁸ o los que la analizan como un apéndice al documento, un conjunto de aspectos que identifican al autor y una solución dada por las nuevas tecnologías a la necesidad de garantizar jurídicamente las contrataciones realizadas por medios electrónicos,⁹ que le impregna sin lugar a dudas un carácter más ágil a estas operaciones comerciales.

Al tener en cuenta la visión teórica que existe sobre la firma en su sentido genérico, el aporte significativo de cada definición es el enlace al concepto de la voluntad jurídica del agente signante. Si se tiene en cuenta la aserción de que la firma es el trazo peculiar mediante el cual un sujeto consigna su nombre y apellido o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad; ni remotamente puede sostenerse que un código por el cual se encripta un documento digital constituya la firma que requiere la legislación civil. Aunque siempre queda la posibilidad de que las partes, mediante convenio de derecho privado, establezcan las características de un sistema informático por el cual se vincularán electrónicamente, la falta de generalidad de esta norma y la inseguri-

de documentos, *Ámbito jurídico de las tecnologías de la información*, en *Cuadernos de Derecho Judicial*, No. 15, Ed. Escuela Judicial-Consejo General del Poder Judicial, Madrid, 1996, pp. 191-245.

⁶ ALCOVER GARAU, GUILLERMO. “Concepto de firma electrónica, firma electrónica y firma manual”, en *Comentarios a la Legislación Concursal*, Dykinson, Madrid, 2000, p. 33.

⁷ MUÑOZ ROLDÁN, LUIS RODRIGO. “El tráfico jurídico electrónico y la firma digital”, en *Panorama actual del derecho notarial en Hispanoamérica (libro homenaje a Isidoro Lora-Tamayo Rodríguez)*, Júpiter, Madrid, 2005, p. 45.

⁸ Véase DELPIAZZO, CARLOS. “De la firma manuscrita a la firma electrónica: un caso de impacto de la tecnología sobre el derecho”, en *Revista de Antiguos Alumnos del I.E.E.M.*, enero de 1998, disponible en <http://inza.wordpress.com/2007/03/24/digitalizacion-de-firma/> [consultada: 26. Marzo. 2012].

⁹ Véase ORMAZÁBAL SÁNCHEZ, GUILLERMO, “El valor probatorio del documento signado en forma digital”, en *Revista a la Llei de Catalunya*, Barcelona, No. 216, 2000, p. 15.

dad jurídica que sugiere el uso de medios no contemplados por la ley obstaculiza el desarrollo de esta nueva tecnología de firma electrónica.

La concepción de la firma manuscrita como el signo que refleja la voluntad del agente signante resulta pertinente para el evaluar el tema en el ambiente digital, y esbozar la firma electrónica como el trazo o signo consiste en una señal digital representada por una cadena de bits, las huellas digitales exportadas al pie del escrito, o simplemente el código o clave en un sistema informático. Pero la observación esencial que se deriva de los conceptos radica que mediante estos signos, claves o huellas, el autor manifiesta su voluntad, vital para enfocar el *animus probandi* que brinda autenticidad y confidencialidad a la información esbozada en el documento.

Así, con la expresión “firma electrónica” se alude a un conjunto heterogéneo de mecanismos electrónicos de autenticación, que van desde la mera inclusión del nombre o la firma manuscrita digitalizada al final del documento hasta los más complejos procedimientos de cifrado y descifrado de datos a partir de un par de claves asimétricas. Pero la idea que se acoge en la tesis es considerar la firma electrónica como el conjunto de datos o signos en forma electrónica consignados lógicamente a un mensaje de datos, y que al ser sometidos a un proceso técnico-matemático de verificación puede primeramente identificar al titular del mensaje y, segundo, dar fe de su integridad y autenticidad. *A priori* de emitir una valoración por la autora, resulta acertado preguntarse ¿cualquier instrumento que reúna estas características mencionadas, es firma electrónica a los efectos de autenticidad?

Por el contrario, no es firma electrónica cualquier medida de seguridad que se encamine a salvaguardar el control sobre el medio de autenticación (llave de la habitación en la que se encuentra el ordenador, tarjeta que contiene los datos de creación de firma, etcétera), pues no tiene carácter electrónico. Igualmente, tampoco es firma electrónica el rastro electrónico que, sin intención por parte del firmante de firmar el documento, quede registrado en relación con el documento electrónico o en el ordenador del emisor, el intermediario o el destinatario de la comunicación.¹⁰

Asimismo, y por faltar también la finalidad de autenticación, no es firma electrónica la utilización del cifrado de datos, sin la intención de identificarse como suscriptor del mensaje. Por ejemplo, el cifrado simétrico de los datos puede utilizarse por varios sujetos sólo para salvaguardar la confidencialidad de las comunicaciones, firmándose además el mensaje mediante otro procedimiento. Y,

¹⁰ Ciertamente en caso de litigio ello podrá ser objeto de una prueba pericial o, en su caso, de reconocimiento judicial, para probar la identidad del emisor y que el documento era conocido y querido por el mismo. Pero la autenticación supone la manifestación consciente de una persona de asumir como propio el contenido de un mensaje.

por último, puede no ser tampoco firma electrónica la utilización de un PIN o del par “nombre de usuario/clave de acceso” cuando sirva a una persona sólo para identificarse, pero relacionado con un mensaje electrónico.

Para esclarecer tal situación, valido remitirse al matiz normativo que establece la Ley Modelo en su artículo 2 a) sobre qué se entenderá por firma electrónica.¹¹ Esta noción que se aborda en la legislación aspira a englobar todos los usos cotidianos de una firma manuscrita con consecuencias jurídicas; es la identificación del firmante y la intención de firmar sólo el mínimo común denominador de los diversos criterios relativos a la “firma” que se aciertan en los diversos ordenamientos jurídicos. La definición no renuncia al hecho que las tecnologías comúnmente señaladas “firmas electrónicas” sabrían utilizarse para otros fines que crear una firma jurídicamente eficaz. La axioma se circunscribe a ilustrar que la Ley Modelo se centra en el uso de firmas electrónicas como equivalentes funcionales de las manuscritas (véase el documento A/CN.9/483, párrafo 62). Para no introducir o sugerir limitaciones técnicas que afectaran el método que el firmante pudiera utilizar para realizar la función equivalente a la firma manuscrita se prefirió emplear palabras flexibles como “datos que puedan ser utilizados”, en vez de referencias a los medios “técnicamente capaces” del firmante.

Otro punto esencial a debatir en cuanto a la nebulosa percepción es en relación con los juicios perpetrados por el dogmatismo. Si bien es cierto que en sus inicios se admitía una categoría genérica del término firma electrónica, existen quienes a la hora de delimitarla realizan una distinción entre firma electrónica simple o básica¹² y firma electrónica avanzada (conocida en la práctica como firma digital).¹³

¹¹ Según el artículo 2. Por “firma electrónica” se entenderá los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el titular de la firma aprueba la información contenida en el mensaje de datos.

¹² La firma electrónica simple (FES) es el conjunto de datos electrónicos que permiten la identificación formal del autor o autores. Son las llamadas firmas comerciales, de pocas garantías y bajo precio, las cuales pueden pertenecer a uno o varios autores. Es un mecanismo tecnológico que permite identificar al usuario cuando realice trámites a través de Internet o redes cerradas. A pesar de que su finalidad es la de identificar al firmante, lo único que manifiesta es la autenticidad del mensaje. Ejemplos de firma electrónica simple son los números de identificación personal (NIP) como llave que se comparte con el banco para hacer transacciones con cajeros automáticos o a través de Internet, la clave para entrar a la cuenta de correo electrónico (de la que toma parte el prestador de servicio) o a alguna biblioteca virtual, así como las contraseñas que se utilizan para el acceso a otros servicios en Internet. La firma simple o básica es reconocida por las primeras legislaciones de los países que siguieron la línea de la ley modelo. Así, es bueno citar el Real Decreto No. 14/1999, de España, que en su artículo 2 c) recogía este tipo de firma electrónica, citando al respecto que la firma electrónica es aquel conjunto de datos técnicos que permiten identificar al sujeto que firma, es decir, al signatario en términos legales. Este Decreto-Ley fue modificado por la Ley No. 59/2003, sobre firma electrónica, la cual reconoce de forma similar la firma electrónica simple. Ley No. 59/2003, del 19 de diciembre de 2003, de firma electrónica. *Boletín Oficial Electrónico* del 20 de diciembre de 2003 (en adelante LFE).

¹³ La firma electrónica avanzada (FEA) es aquella que permite lograr la identificación del firmante y verificar la au-

Una adecuación a este pensamiento se procesó en el ámbito teórico-normativo español; en este sentido, se establece por la legislación foránea la existencia de dos modalidades de la institución, centrándose el mayor debate en la firma electrónica avanzada.¹⁴ De esta forma define que la firma electrónica es “el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”; por su parte, en el apartado 2 se introduce el concepto de firma electrónica avanzada, caracterizándola por ser la que permite la identificación del signatario y el hecho de ser creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente con él y con los datos que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

De las dos definiciones expuestas se considera que la correspondiente a la llamada firma electrónica no se ajusta a las cualidades procuradas como propias de este mecanismo para garantizar autenticidad al documento. Al asumir este concepto cabrían equívocas fórmulas como la inclusión de un simple nombre, una contraseña o la reproducción digitalizada de la firma autógrafa¹⁵ y, por supuesto, otras técnicas algo más sofisticadas, pero que sólo impropriadamente pueden calificarse como tales, como son las basadas en datos biométricos, *pins* o *passwords*. La inserción de este ambiguo e impropio significado se critica por el exceso que supone atribuir tal calificación a unos sistemas que no garantizan la integridad del contenido asociado, y que sólo se utiliza por un sector económico que comercializa determinados productos bajo la denominación de firma electrónica.¹⁶

Definitivamente, la verdadera firma electrónica, a los efectos de autenticidad del documento, es la que se conoce en la propia LFEE como avanzada,¹⁷ esta en-

tenticidad de los datos firmados, concebida en la mayoría de las legislaciones al respecto, es la más utilizada. Este tipo de firma es utilizado por muchos países de América (México, Ecuador, Estados Unidos, Bolivia, Perú) y Europa (España, Alemania, Francia, Italia), pues garantiza la seguridad de las transacciones electrónicas.

¹⁴ Por ejemplo, LFEE, artículo 3.1.

¹⁵ Véase MARTÍNEZ NADAL, APOLÓNIA. *Comentarios de urgencia al urgentemente aprobado Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica*, 3a. ed. revisada y aumentada, Civitas, Madrid, 2001, p. 2.

¹⁶ Véase ALCOVER GARAU, G. “La firma electrónica como medio de prueba: valoración jurídica de los criptosistemas de claves asimétricas”, en *Cuadernos de Derecho y Comercio*, Consejo General de los Colegios Oficiales de Corredores de Comercio, Madrid, No. 13, abril de 1994, p. 23.

¹⁷ Las diferentes legislaciones hablan de firma digital o de firma electrónica como si se tratara de lo mismo. Algunas legislaciones, como en la española ya citada, o la argentina, legislan sobre firmas digitales, firmas electrónicas y firmas digitales avanzadas. La legislación colombiana como la ecuatoriana legislan sobre el mismo aspecto pero con términos diferentes; es decir, que si en el Ecuador se habla de firma electrónica en Colombia se debe entender a ésta como firma digital. Por otro lado, la legislación peruana tiene un aspecto particular, diferente al de las otras dos legislaciones. El artículo 3 de la Ley No. 27269, dispone: “La firma digital es aquella firma electrónica [...]”; así, se puede notar que el legislador peruano establece una relación género-especie entre estas dos terminologías, en donde firma electrónica sería el término genérico que abarca todo el universo, de modos en que se puede “firmar” un documento electrónico, como lo define el artículo 1. Dentro de ese universo se encuentra la firma digital que es

cierra los elementos que toda firma manuscrita posee: permitir la identificación del signatario y la autenticación del contenido que recoge. Más allá de hablar de firma digital o de firma electrónica, se debe tener claro que el legislador de cada país busca regular la producción, efectos, requisitos, obligaciones, duración y extinción de la firma que cumpla con los requisitos técnicos para garantizar la efectiva integridad, identidad, no repudio y autenticidad de un mensaje de datos, y así resguardar una relación jurídica que es de interés para ese ordenamiento jurídico, como el caso de la contratación y el documento vía electrónica.

No obstante, en legislaciones que la regulan actualmente —a criterio de la autora de la investigación—, la innegable diferencia entre firma digital y firma electrónica se encuentra en el alcance que ofrece cada reglamentación y en el mecanismo de seguridad que se utilice para garantizar sus características. En este sentido, si se parte del hecho de avalar la integridad, autenticidad e identidad de un mensaje, el término firma electrónica (a excepción del Ecuador) se utiliza para regular las formas de firmas que no se enmarcan dentro del sistema de criptografía asimétrico, y el término firma digital para aquellas formas que sí cumplen con los parámetros que implica la utilización de este criptosistema. A efectos de mantener la claridad y la armonía de los conceptos en esta investigación se hablará simplemente de “firma electrónica”.¹⁸

En síntesis, se acoge desde el punto de vista del derecho que la firma electrónica consiste en cualquier símbolo o signo basado en medios electrónicos que utiliza una persona con el objetivo puntual de identificarse, relacionarse y autenticar el contenido de un documento. En otras palabras, es el sustituto de la firma manuscrita que, en el marco del intercambio electrónico de datos, permite al receptor de un mensaje electrónico verificar con certeza la identidad que

la única que para su existencia requiere pasar un proceso técnico matemático o lógico. Existe además otra particularidad dentro de esta legislación; es el hecho de que el legislador peruano, equivocadamente —a juicio de la investigadora—, le otorga a la firma electrónica la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Se dice equivocadamente ya que no todas las formas de “firmar” un documento, o de manifestar la voluntad de los signatarios, han sido generadas a través de procesos técnicos seguros, y por lo tanto vagamente podrían garantizar la integridad del documento o la identificación del signatario. Por este motivo, las legislaciones ecuatoriana y colombiana establecen esta equivalencia legal, solamente a aquellos “modos de firmar” que sean generados mediante procesos técnicos y matemáticos seguros y que puedan garantizar la identidad e integridad de los documentos, criterio que se comparte en la investigación. Véase Ley No. 52, artículo 2 c), de Colombia; Ley No. 2002-67, Ecuador, artículo 13. Asimismo, la Ley No. 27269 del Perú, en su artículo 3.

¹⁸ En toda la investigación se hablará de firma electrónica sin el apellido avanzada, pero se establece que se refiere a este mecanismo que posibilita la seguridad, autenticidad y validez jurídica de los documentos electrónicos, tal como se expresa en la tesis. Se acogen las posiciones adoptadas por las leyes italiana y peruana. Véase Reglamento Italiano, artículo 1 b) y el artículo 2.1 primera parte de la Ley peruana. Para profundizar sobre el término véase RODRIGO ADRADOS, ANTONIO. “Firma electrónica y documento electrónico. Escritura pública”, en *Ensayos de actualidad*, La Ley, España, No. 24, 2004, p. 60; VATIER FUENZALIDA, CARLOS. “El régimen legal de la firma electrónica”, en *Actualidad Civil*, La Ley, Madrid, No. 11, marzo de 2000, p. 412; MARTÍNEZ NADAL, A. *Comercio electrónico, firma digital y entidades de certificación*, Dykinson, Madrid, 1998, p. 45.

proclama el trasmisor, e impide a este último desconocer la autoría del mensaje en forma posterior.

En un matiz técnico, es la transformación de un mensaje donde se emplea un sistema de cifrado asimétrico, es decir, son unas claves criptográficas asimétricas en las que se combinan claves —pública (que se enviará al o los destinatarios para que sean capaces de recibirlo y autenticar su identidad) y privada (para la utilización personal e intransferible del solicitante)— que encriptan el documento e impiden su manipulación y su conocimiento público. Resulta, por tanto, ser la herramienta que permite determinar de forma fiable si las partes que intervienen en una transacción son las que realmente dicen ser, que garantiza la confidencialidad, autenticidad e integridad de los mensajes contenidos en la transacción.

Es así que se aprecia que es un instrumento con características técnicas y normativas, lo que significa que existen documentos legales que respaldan no sólo su acepción, sino además el valor nomotético que ella posee, y procedimientos experimentados que permiten la creación y verificación de éstas. Sobre estos aspectos preceptivos se expone en los siguientes epígrafes.

2. Labor unificadora de la firma electrónica en el marco de las Naciones Unidas y estatal

Efectivamente, el comercio electrónico genera también incertidumbres derivadas de la misma naturaleza de los medios a través de los que este comercio se desenvuelve, y que plantean problemas de autenticación, integridad, rechazo y confidencialidad de las comunicaciones. Mientras desde el punto de vista técnico existen ya medios e instrumentos para solventar estos últimos problemas, desde el punto de vista jurídico, el estado actual de las leyes presenta todavía importantes incertidumbres que generan dudas importantes sobre la validez y eficacia de las transacciones electrónicas.

En los últimos años se detecta una actividad notable en la regulación de múltiples aspectos de las nuevas tecnologías en general, y, por lo que ahora interesa, del problema de la autenticidad y el no rechazo en destino. A continuación se exponen algunas regulaciones, sin ánimo de ser exhaustivos, pues pueden encontrarse otras disposiciones relativas a notificaciones electrónicas, registros telemáticos, entre otras, pero sí con la intención de exponer las más relevantes y significativas a nivel internacional y estatal que contribuyen a garantizar la seguridad y fiabilidad de las transacciones electrónicas.

Desde el punto de vista jurídico, y en primer lugar en las iniciativas internacionales que debe ser el ámbito de partida del tema, la norma marco desarrollada

por la CNUDMI entró en vigor en 2001 con su Guía para la Incorporación al Derecho Interno, y fue la primera disposición sobre la materia con la que se contó en el plano internacional y a la cual se acogieron diferentes Estados en idéntico sentido que la Ley Modelo de Comercio Electrónico.

La ley recoge la aplicación en los casos en los que se utilice la firma electrónica en actividades comerciales, lo que se señala en la propia norma de forma clara y precisa.¹⁹ Entre sus principales características establece un conjunto de definiciones, tal es el caso de mensajes de datos, firma electrónica, certificados, firmantes y parte que confía, así como las obligaciones de cada parte; instaura los mecanismos de certificados digitales desarrollados por las entidades de certificación, y admite la posibilidad de los certificados digitales y firma electrónica emitida por entidades extranjeras. Elemento interesante en cuanto al particular es la eventualidad de equiparación de la firma electrónica con la firma manuscrita, por lo que enuncia los elementos a tenerse en cuenta en tal paralelo.²⁰ Aunado a estas prácticas legislativas internacionales, se han establecido documentos orientativos elaborados por grupos privados, tal es el caso del *ABA Digital Signature Guidelines*, así la *American Bar Association* ha desarrollado un modelo de directrices o líneas básicas sobre firma digitales a través del trabajo de la *ABA Science and Technology Section's Information Security Committee*. Por otro lado, se resalta la labor desarrollada por la Cámara de Comercio Internacional, quien aprobó el *General Usage for International Digitally Ensured Commerce* —GUIDEC—, cuyo principal objetivo es establecer el marco general para la seguridad y certificación de mensajes digitales, teniendo en cuenta que se presupone que las

¹⁹ "La Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [...]".

²⁰ Artículo 6. "Cumplimiento del requisito de firma

1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.

2. El párrafo 1 será aplicable tanto si el requisito a que se refiere está expresado en forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3. La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1 si:

- a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
- b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
- c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y
- d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

4. Lo dispuesto en el párrafo 3 se entenderá sin perjuicio de la posibilidad de que cualquier persona:

- a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1, la fiabilidad de una firma electrónica; o
- b) aduzca pruebas de que una firma electrónica no es fiable".

partes son expertos empresarios o profesionales que actúan bajo la *lex mercatoria*, por lo que se excluyen las transacciones con consumidores.

La adopción, por diferentes Estados, de los lineamientos de la Ley Modelo en disímiles formas y alcances resulta un patrón a seguir para definir un marco internacional uniforme para el comercio electrónico. En el ámbito interno, los pioneros en regular esta materia fueron los norteamericanos.²¹ En dicho país, a pesar de existir regulaciones a nivel estatal, sin existir uniformidad entre las diferentes normas, se extraen particularidades comunes, que se reducen a tres: la voluntariedad del sistema, la equivalencia del documento electrónico y el escrito convencional y la equivalencia de la firma electrónica con la firma escrita. Washington adopta una legislación muy parecida en 1996, y otros Estados, como Georgia, empiezan a ver la Ley de Utah como modelo.

A pesar de mantenerse este pensamiento en algunos Estados, de mantener la Ley de Utah como modelo, otros prefieren sistemas menos reguladores y no tan tecnológicos, cabe señalar a California y Arizona, quienes han aprobado legislaciones que permiten el uso de firmas digitales para transacciones con las entidades públicas de cada Estado, autorizando al secretario de Estado a dictar normas para alcanzar la finalidad de la ley; otros tienen leyes que permiten el uso de firmas electrónicas con finalidades específicas médicas (Connecticut) o financieras (Delaware), de igual forma existen nuevas tendencias.²²

Los países del Continente europeo no estuvieron al margen, así en la Unión Europea se comenzó a regular la firma electrónica a nivel comunitario con la Directiva 1999/93 sobre firma electrónica, la cual implanta un concepto sobre el término “los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación”.²³ Con anterioridad a la Directiva, e incluso a la propia Ley Modelo, Alemania e Italia legislaron en materia de firma electrónica.

²¹ La primera ley a nivel de país fue la Ley del Estado de Utah sobre firma digital, Código Comentado. Título 46, Capítulo 3 (1996) referenciada conforme normas de la American Bar Association (ABA) (versión corregida-diciembre de 1996). El texto completo en castellano está en <http://www.cnv.gov.ar/FirmasDig/Internacional/lutah.html>. Ésta marcó un precedente para otras leyes americanas estatales, así como de leyes de otros países, como Alemania, Francia, Argentina, y la propia Unión Europea. Véase RICHARD, JASON. “The Digital UTA Signature Act As Model Legislation: A Critical Analysis”, en *Journal of Computer & International Law*, vol. XVII, No. 3, 1999, pp. 873-907.

²² Refiérase el estado de Massachusetts, que da efecto legal a las firmas y documentos electrónicos, no sólo las firmas digitales, teniendo en cuenta la naturaleza dinámica e impredecible de la evolución tecnológica. Cítese de igual forma la *Florida Electronic Signature Act* de 1996, que tiene como objetivo el desarrollo del comercio electrónico en el sector público y privado, y da a las firmas electrónicas la misma fuerza y efectos que las firmas manuales, de forma que todos los tipos de firmas electrónicas existentes y futuras, incluidas las firmas digitales, son ahora iguales legalmente a las firmas manuscritas.

²³ Véase Directiva Europea 1999/93 sobre la firma electrónica, Parlamento Europeo y del Consejo, del 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica, artículo 2.1. Tal criterio es seguido en la LFEI, artículo 3.1. Sin duda alguna ambos artículos no son claros en su conceptualización debido a que no abordan la naturaleza de la firma electrónica, por eso el resultado conceptual es relativamente neutro.

La ley alemana,²⁴ a pesar de crear un marco de condiciones para la institución, bajo las cuales éstas pueden considerarse seguras, de manera que se pueda determinar con una innegable seguridad cuándo una firma es falsificada o cuándo unos datos firmados mediante firma electrónica son manipulados, se critica por la autora que no regule los aspectos civiles de éstas, no equipara el documento en soporte informático al de soporte de papel, ni identifica los efectos del documento firmado de forma manuscrita a la firma por medios digitales, además de sólo ocuparse de la firma electrónica, sin entrar en el tema del cifrado de los documentos informáticos.

En Italia,²⁵ de forma similar a la legislación alemana, se establece un marco formal para su utilización y se valora el deber de asesoramiento que necesita el certificador, aunque de forma más contundente y novedosa el Reglamento italiano; además, se instituye que el certificador no puede hacerse depositario de las llaves privadas, y luego regula por separado la posibilidad de su depósito en otras instancias, criterio con el que se está en desacuerdo, al ser éste un elemento esencial para garantizar la total seguridad de las firmas electrónicas.

Otro punto discordante y novel es regulado en el artículo 16 del Reglamento italiano, el cual legaliza la firma electrónica autenticada, cuya oposición sea certificada por notario u otro oficial público autorizado, y le proporciona al primero la facultad de asegurarse de la identidad del firmante, tal como lo regula el cc al respecto (*cf.* artículo 2703, Código Civil italiano); incluso más allá que el anterior, al exigir que se asegure igualmente la validez de la llave pública y del hecho de que el documento firmado responde a la voluntad del firmante y no es contrario al ordenamiento jurídico.

Las leyes alemana e italiana, conformes con esta realidad, formalmente se refieren al procedimiento técnico de dualidad de clave asimétrica, privada y pública, con lo que proporcionan más transparencia y seguridad al sistema, aunque con el incuestionable riesgo de resultar obsoletas por el ascenso tecnológico. Sin embargo, no indican nada acerca de la firma electrónica avanzada, y dejan al margen aquellas firmas suscitadas por otros procedimientos técnicos (Alemania), o les reconocen menores efectos (Italia).

En España han existido, en los últimos tiempos, distintas iniciativas legislativas sobre esta materia, desde normativas autonómicas, concretamente regula-

²⁴ Ley de firmas digitales, aprobada por el Bundestag el 13 de junio de 1997, Teil I Seite 1872-6 y Reglamento Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Bundesgesetzblatt - BGBl. Teil I s. 876 vom 21. Mai 2001, Published 16 may 2001. Official Journal No. 22, 22 may 2001. In Forcé 22 may 2001. Esta ley forma parte de una ley más amplia, denominada Ley Multimedia, que regula con carácter general las condiciones de los servicios de información y comunicaciones.

²⁵ Véase Reglamento italiano.

doras de la firma electrónica en el ámbito de la administración pública;²⁶ como normas en la administración central u otras reguladoras de la utilización de la firma electrónica por parte de registradores y notarios,²⁷ y culmina su proceso legislativo con la aprobación de la LFEE, cuya finalidad se enmarca en reforzar el marco jurídico existente, e incorpora en su texto algunas novedades con respecto a su antecedente inmediato, el Real Decreto —Ley 14 de 1999—.²⁸

Pues bien, la LFEE, igual que la directiva de la que trae causa, aborda únicamente la regulación de la firma electrónica como elemento que, junto con el sistema de certificados, permite solucionar los ya mencionados problemas de autoría, integridad y no rechazo en origen, que se originan en los medios electrónicos a través de los que se desarrollan las comunicaciones comerciales, y para los que se ha ofrecido una solución técnica y jurídica.

Los países latinoamericanos, de acuerdo a los avances tecnológicos, se encuentran en correspondencia con el criterio de la Ley Modelo, de la Directiva Europea o de la propia Ley de Utah, entre ellos se destacan Argentina,²⁹ Perú,³⁰

²⁶ V. gr. Decreto Ley 205 del 3 de diciembre de 2001 por el que se regula el empleo de la firma electrónica en los procedimientos administrativos de la Comunidad Autónoma de Canaria; la Ley 3, del 21 de mayo de 2002, para el desarrollo del uso de la firma electrónica en las administraciones públicas de la Comunidad Autónoma de la Rioja, y el Decreto 87, del 30 de mayo de 2002, del gobierno valenciano, por el cual se regula la utilización de la firma electrónica avanzada en la Generalitat valenciana. Véase MARTÍNEZ NADAL, A. *Comentarios a la Ley 59/2003 de Firma Electrónica*, Civitas, Madrid, 2004, p. 25.

²⁷ V. gr. Orden del 26 de diciembre de 2001 por la que se establecen los criterios generales de tramitación telemática de determinados procedimientos por el Ministerio de Economía y los organismos públicos adscritos al departamento y se crea un registro telemático para la presentación de escritos y solicitudes, y la Ley 24, del 27 de diciembre de 2001, de medidas fiscales, administrativas y del orden social. Véase *idem*.

²⁸ El Real Decreto Ley 14, del 17 de septiembre de 1999, sobre firma electrónica fue aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad empresarial, los ciudadanos y las administraciones públicas. Pero esta normativa decayó con la expiración del mandato de las cámaras en marzo de 2000, por lo que la presente legislación sobre la temática resulta ser el resultado del compromiso asumido en la VI Legislatura que actualiza el Real Decreto Ley mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor tanto en el país como a nivel internacional.

²⁹ El marco normativo de la República Argentina en materia de firma electrónica está constituido no sólo por la Ley No. 25.506 (*Boletín Oficial* del 14 de diciembre de 2001), sino también por el Decreto No. 2628/02 (*Boletín Oficial* del 20 de diciembre de 2002) y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos. La aparición de esta ley provocó un vuelco en la forma de los actos jurídicos mediante el reconocimiento de los documentos digitales y el valor probatorio que detentan, provocando una modificación tácita en las disposiciones del Código Civil en materia de instrumentos públicos. La ley se creó con la finalidad de eliminar los prejuicios en relación con este tipo de documento, y así dilucidar si puede considerarse que el texto inserto en un soporte distinto al papel cumple con el requisito de la escritura.

³⁰ Ley No. 27.269 de 2000. El modelo de ley peruano de forma satisfactoria define la validez y eficacia de las firmas digitales y documentos electrónicos y los expresa en los artículos 3 y 4. Esta ley legisla el uso de estos medios como forma efectiva de despapelización de la sociedad y como medio de desarrollo, siendo una de las más avanzadas en estos temas dentro de los países latinoamericanos. Ley No. 27.269, Ley de Firmas y Certificados Digitales, Perú, promulgada el 26 de mayo de 2000, publicada en el *Diario Oficial el Perú* el 28 de mayo de 2000.

Colombia,³¹ Costa Rica,³² Chile,³³ México,³⁴ Venezuela,³⁵ sólo por mencionar algunos.³⁶

En los heterogéneos cuerpos normativos se acoge la posición de que la firma sirve para identificar al firmante y, en consecuencia, cumple un papel análogo a la firma manuscrita, por lo que validan la equivalencia funcional entre estas tipologías. En el orden semántico habría que hacer la precisión de que la firma electrónica no se apoya en la idea de ser, en cuanto a la confección de puño y letra, del autor, aunque sirve para reflejar la autoría de un documento. Algunas leyes al respecto impulsan el uso voluntario, y otras generalizado, de la firma electrónica en la actividad económica y social, abogan por la existencia de los certificados digitales con sus correspondientes entidades de certificación.

Finalmente, resulta certero mencionar la existencia de las denominadas declaraciones de prácticas de certificación,³⁷ compendio del régimen aplicable y

³¹ Ley No. 527 de 1999 de Mensaje de datos, Colombia, publicado en el *Diario Oficial*, No. 43.673, del 21 de agosto de 1999. Sin embargo, existen normas previas que hacen relación a temas electrónicos como la Ley 270 de 1996 – Estatutaria de la Administración de Justicia y el Decreto 1094 de 1996 que reglamentó el artículo 617 del Estatuto Tributario con el fin de regular las condiciones y mecanismos del sistema de facturación electrónica. Posteriormente, en 2007 se estableció el Decreto 1929 de 2007 y la Resolución 14465 del 28 de noviembre de 2007, ambas sobre Facturación Electrónica. Disponibles en http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2007/decreto.html [consultado: 25. Noviembre. 2012].

³² Ley No. 8454 del 30 de agosto de 2005, Ley de certificados, firmas digitales y documentos electrónicos de Costa Rica. Publicada en la *Gaceta No. 197*, del 13 de octubre de 2005.

³³ Ley 19.799 de 2002, Ley sobre firma electrónica de Chile. Promulgada el 26 de marzo de 2002. Publicada en el *Diario Oficial* el 12 de abril de 2002.

³⁴ Decreto por el que se expide la Ley de Firma Electrónica Avanzada. México, Distrito Federal, promulgada el 24 de noviembre de 2011; expidió el presente Decreto en la Residencia del Poder Ejecutivo Federal, en la Ciudad de México, Distrito Federal, a seis de enero de dos mil doce, publicada en el *Diario Oficial de la Federación* del 11 de enero de 2012. Disponible en http://dof.gob.mx/nota_detalle.php?codigo=5228864&fecha=11/01/2012 [consultada: 5. Septiembre. 2012].

³⁵ Decreto con Fuerza de Ley No. 1.181 del 17 de enero de 2001, sobre mensajes de datos y firmas electrónicas, Venezuela, publicado en *Gaceta Oficial de la República Bolivariana de Venezuela*, No. 37.148, del 28 de febrero de 2001. Legislada en el marco de la Ley Habilitante otorgada por el presidente de la República Bolivariana de Venezuela.

³⁶ Ley No. 18.600 del 21 de septiembre de 2009 sobre el documento electrónico y firma electrónica de Uruguay, publicada en el *Diario Oficial de la República Oriental de Uruguay*, No. 5 del 5 de noviembre de 2009, y Decreto No. 450/2009 del 28 de septiembre de 2009 sobre el gobierno electrónico en red, República Oriental del Uruguay; Ley No. 4017/2010 del 23 de diciembre de 2010, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico, publicada en la *Gaceta Oficial de la República del Paraguay*, No. 252, del 24 de diciembre de 2010, y Decreto 7369/2011 del 23 septiembre de 2011, que aprueba el Reglamento General de la Ley 4017/2010 de Validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico, disponibles en <http://www.informatica-juridica.com/legislacion/> [consultadas: 3. Septiembre. 2012]; Ley 067 de 2002 sobre comercio electrónico, firma electrónica y mensajes de datos de Ecuador y su respectivo reglamento de aplicación, publicada en el *Registro Oficial*, Suplemento No. 577 del 17 de abril de 2002; Ley No. 729, "Ley de Firma Electrónica", Nicaragua, publicada en la *Gaceta Diario Oficial* el 30 de agosto de 2010.

³⁷ Una declaración de prácticas de certificación es aquel documento en que la autoridad de certificación establece su política de actuación, y las prácticas que aplica en la emisión de sus certificados, y en los distintos momentos posteriores de distribución, suspensión, revocación y expiración del mismo. Éstas pueden tener la forma de declaración de la autoridad, puede ser un estatuto o regulación de la misma, o un estatuto o regulación de la misma,

aplicado por una autoridad de certificación en el sistema de certificados, que constituyen una importante fuente no legal pero sí fruto de la autonomía de la voluntad. Estas prácticas pueden plantear algunos problemas,³⁸ y en remisión a éstos establecen que, cuando se modifique su contenido, los suscriptores de certificados vigentes deberán aceptar el nuevo contenido o proceder a solicitar la revocación de los certificados en un determinado periodo, transcurrido el cual, sin actuación alguna del suscriptor, se entenderá que aceptan implícitamente.³⁹

3. La futura ley cubana

En cuanto a una normativa reguladora de la firma electrónica en Cuba, aún no se cuenta con una legislación al respecto, se elaboraron algunos proyectos de decreto-ley basándose principalmente en las legislaciones de la UNCITRAL, de Argentina, Colombia, Perú, Alemania e Italia. Su última versión es el Proyecto cubano de PKI, el cual establece que la firma electrónica es “el resultado de aplicar a un documento digital un procedimiento informático criptográfico que garantiza su integridad y autenticidad”.⁴⁰ Si bien éste expresa un concepto de forma similar a lo establecido en la legislación argentina, y asienta de manera acertada el mecanismo a utilizar, como es el criptográfico, sin precisar el tipo; se increpa el no establecer una definición acorde con la doctrina científica, en correspondencia con los caracteres que desde el orden doctrinal la integran. De igual forma, no brinda una explicación eficaz de los elementos importantes que la teoría engloba en la definición de tradicional, como es la identidad del autor y la integridad del mensaje, sólo menciona la necesidad de garantizarlos.

No obstante, el proyecto expone cuestiones esenciales sobre el tema, como es el caso de la equivalencia entre el soporte de papel y el electrónico, y el papel

o también parte del contrato entre la autoridad de certificación y el suscriptor. En este sentido, se hace especial pronunciamiento a la incorporación por referencia, concretamente en el derecho español a la Ley 7, del 13 de abril de 1998, sobre condiciones generales de la contratación, que establece, de forma específica, los casos de contratación telefónica o electrónica y plantea remisión reglamentaria respecto de la aceptación de las cláusulas contractuales, así como el contenido y la extensión del justificante escrito del contrato con constancia de todos sus extremos que ha de enviarse al consumidor.

³⁸ Señalan las *ABA Guidelines*, si el mensaje no existe hasta después del tiempo de efecto, o la información del mensaje incorporado ha sido alterado, estos documentos creados o modificados posteriormente no serán considerados incorporados por referencia.

³⁹ Por ejemplo, las declaraciones de prácticas de certificación de *Verisign Inc.* prevén su posible modificación, en cuyo caso las modificaciones deberán ser publicadas en el repositorio de la autoridad de certificación, y, como regla general, tendrán efecto a los 15 días de esa publicación. De igual forma, se establece que dentro del término de 15 días si el suscriptor no revoca el certificado se tiene por conforme con la enmienda o modificación.

⁴⁰ Proyecto de Decreto-Ley cubano de PKI, “Propuestas de bases legales para establecer, organizar y desarrollar una infraestructura de llave pública en Cuba”, última versión del 8 de febrero de 2008, artículo 63, apartado 1.

de las entidades de certificación en la verificación de las firmas, y a diferencia de las legislaciones que sobre el tema existen tanto a nivel internacional como de Estados, es mucho más abarcador, porque no se limita, como la mayoría de estas regulaciones, a operaciones comerciales, sino que su ámbito de aplicación es más amplio, comprende operaciones o transacciones de cualquier índole que se realicen por los medios electrónicos, con las excepciones que establece el cuerpo de la norma o las que se infieren de su propia naturaleza (véase artículo 1). En este sentido, resulta adecuada la manera en la que engloba toda la infraestructura de firma electrónica, elementos que la hacen más viable para la implementación del mecanismo en Cuba, lo que no excluye la necesidad de realizarle algunas modificaciones encaminadas precisamente al procedimiento que garantice validez y autenticidad de los documentos electrónicos. No obstante —a criterio de la autora—, la definición que se expone de firma electrónica es muy engorrosa o poco clara a pesar de que sigue la tendencia del derecho comparado en orden a referirse al contenido de la firma y su relación con la entidad certificadora, y subyace en ella la existencia de un mecanismo asimétrico de llaves.

Se considera acertado enumerar que el proyecto no promueve, de forma general, las reglas de estandarización de los documentos electrónicos, ni establece las normas de responsabilidad penal, así como las contravenciones y multas para el caso del mal uso de la firma electrónica que generaría un problema de falsedad. Se pondera que se dedique una sección a los términos, condiciones y requisitos en que se hacen las firmas electrónicas; unicidad de generación de datos, imposibilidad de falsificación tecnológica, integración al mensaje de datos, uso como elemento de convicción en caso de procesos judiciales.

En otro orden normativo, el proyecto cubano sobre comercio electrónico a la hora de mencionar la forma mediante la cual se trasmite y recibe el mensaje de datos expresa la vinculación del emisor con éste a partir de la utilización de un medio de identificación legalmente establecido (véase artículo 6.1), sin hacer alusión a la firma. El objetivo de tal proyecto era ir mucho más allá de las prácticas de comercio electrónico, de ahí que valore la validez del mensaje, y siga idéntica filosofía que la LMCE, por eso se plantea que la firma es un instrumento de autenticidad que implica importancia y encierra el resto de los elementos que garantizan la validez. Resulta conveniente comentar que la certificación a que se refiere el decreto-ley no excluye el cumplimiento de las formalidades de registro público o autenticación que de conformidad con la ley requieren determinados actos o negocios jurídicos; para siempre dejar la posibilidad de que en algunos casos (por su importe, por el tipo de negocio, por los participantes en la relación comercial, por leyes de terceros países involucrados, entre otros) se pueda exigir la autenticación oficial.

Por consecuencia, la legislación que se estipule sobre firma electrónica debe recoger todos los elementos necesarios para brindarle total seguridad, confidencialidad y autenticidad a las transacciones que se realizan a través de la red.

4. A manera de conclusión

La problemática en cuanto a los contratos vía electrónica y el documento electrónico reside en el vacío de garantías a las que están sujetas las partes, situación encabezada por la inseguridad y no autenticidad que significa la no existencia de una firma escrita para su perfeccionamiento. Sin embargo, éstas están suplidas por los avances tecnológicos que signaron la aparición de la firma electrónica.

La falta de regulación y estandarización legal puede ser un obstáculo al desarrollo del comercio electrónico seguro, de ahí la necesidad de un estándar internacional y nacional para determinar qué garantiza o asegura la firma electrónica.

La necesidad de mínimas normas internacionales para el reconocimiento de las firmas electrónicas, los certificados digitales y las prácticas de certificación resultan indispensables en la medida en que el comercio deviene más internacional y universal.

A nivel internacional, la utilización de la firma electrónica es el nuevo medio para dar autenticidad al documento electrónico, regulado de forma cosmopolita por la mayoría de los Estados que la han acogido. En el caso de Cuba, la aceptación de nuevos mecanismos de autenticación, como lo constituye la firma electrónica, requiere la promulgación de una legislación para otorgarle validez y establecer mayor certeza jurídica en cuanto a su eficacia. ■