Naciones Unidas A/CN.9/630/Add.2

Asamblea General

Distr. general
26 de abril de 2007
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
40º período de sesiones
Viena, 25 de junio a 12 de julio de 2007

Posible labor futura en la esfera del comercio electrónico

Documento general de consulta relativo a los elementos necesarios para establecer un marco jurídico favorable al comercio electrónico: modelo de capítulo sobre la utilización internacional de métodos de autenticación y firma electrónicas

Nota de la Secretaría*

Adición

En el anexo de la presente nota figura parte de un modelo de capítulo (primera parte, cap. II, seccs. A y B) de un documento general de consulta que se ocupa de las cuestiones jurídicas relacionadas con la utilización internacional de métodos de autenticación y firma electrónicas.

* La presentación del presente documento por la Secretaría de la Comisión de las Naciones Unidas para el derecho mercantil internacional se retrasó debido a la falta de personal.

V.07-82830 (S) 240507 250507

Anexo

Índice

Primera parte
Métodos de autenticación y firma electrónicas

[...]

II. Trato jurídico de la autenticación y las firmas electrónicas

1. La creación de confianza en el comercio electrónico reviste gran importancia para su desarrollo. Tal vez se precisen normas especiales para aumentar la certidumbre y la seguridad en su utilización. Dichas reglas podrán estar previstas en una diversidad de textos legislativos: instrumentos jurídicos internacionales (tratados, convenios y convenciones); leyes modelo transnacionales; legislación interna (basada a menudo en leyes modelo); instrumentos de autorreglamentación[1]; o acuerdos contractuales[2].

2. Un volumen importante de operaciones comerciales electrónicas se lleva a cabo en redes cerradas, es decir, grupos con un número limitado de participantes a los que pueden acceder únicamente personas o empresas previamente autorizadas. Las redes cerradas apoyan el funcionamiento de una sola entidad o de un grupo de usuarios cerrado ya existente, como las instituciones financieras participantes en el sistema de pagos interbancarios, las bolsas de valores y productos básicos, o una asociación de líneas aéreas y agencias de viajes. En tales casos, la participación en la red se suele restringir a instituciones y empresas admitidas previamente en el grupo. La mayoría de dichas redes han existido desde hace varios decenios, emplean tecnología muy avanzada y han adquirido un alto nivel de pericia en el funcionamiento del sistema. El rápido crecimiento del comercio electrónico en el último decenio ha dado lugar a la aparición de otros modelos de redes, como las cadenas de suministro o las plataformas comerciales.

3. Aunque estos nuevos grupos se estructuraron en un principio alrededor de conexiones directas de computadora a computadora, como ocurría en el caso de la mayoría de las redes cerradas que ya existían en esa época, se da la creciente tendencia de utilizar medios accesibles públicamente, como Internet, en calidad de medio común de conexión. Una red cerrada mantiene su carácter exclusivo incluso en el marco de estos modelos más recientes. Por lo general, las redes cerradas funcionan con arreglo a normas, acuerdos, procedimientos y reglas contractuales

---

[1] Véase, por ejemplo, Comisión Económica para Europa, Centro de las Naciones Unidas para la Facilitación del Comercio y el Comercio Electrónico, recomendación Nº 32, titulada "E-commerce self-regulatory instruments (codes of conduct)" (ECE/TRADE/277), disponible en http://www.unece.org/cefact/recommendations/rec_index.htm, consultada el 28 de marzo de 2007.

[2] Existen muchas iniciativas en los planos nacional e internacional encaminadas a elaborar contratos modelo. Véase, por ejemplo, Comisión Económica para Europa, Grupo de Trabajo sobre facilitación de los procedimientos comerciales internacionales, recomendación Nº 26, titulada "The commercial use of interchange agreements for electronic data interchange" (TRADE/WP.4/R.1133/Rev.1); y Centro de las Naciones Unidas para la Facilitación del Comercio y el Comercio Electrónico, recomendación Nº 31, titulada "Electronic commerce agreement" (ECE/TRADE/257), ambas disponibles en http://www.unece.org/cefact/recommendations/rec_index.htm, consultadas el 28 de marzo de 2007.

convenidos previamente que reciben distintas denominaciones, como “reglas del sistema”, “reglas de funcionamiento” o “acuerdos entre socios comerciales”, concebidos para proporcionar y garantizar a los miembros del grupo la funcionalidad, fiabilidad y seguridad operacionales necesarias. Dichas reglas y acuerdos suelen ocuparse de asuntos como el reconocimiento del valor jurídico de las comunicaciones electrónicas, el momento y el lugar del envío o la recepción de mensajes de datos, los procedimientos de seguridad para obtener acceso a la red y los métodos de autenticación o firma que han de utilizar las partes[3]. Dentro de los límites de la libertad contractual que prevé el derecho aplicable, dichos acuerdos y reglas suelen disponer de un mecanismo de autocontrol.

4. No obstante, si no existen reglas contractuales, o en la medida en que el derecho aplicable pueda limitar su ejecutoriedad, el valor jurídico de los métodos de autenticación y firma electrónicas que utilicen las partes vendrá determinado por las normas de ley aplicables, que pueden ser normas supletorias o de obligado cumplimiento. En el presente capítulo se examinan las diversas opciones a que se recurre en distintos foros para elaborar un marco jurídico para la firma y la autenticación electrónicas.

A. Criterio tecnológico de los textos legislativos

5. La legislación y la reglamentación de la autenticación electrónica han adoptado muchas formas distintas en el plano internacional y el nacional. Cabe señalar tres criterios principales para abordar las tecnologías de firma y autenticación, a saber: a) el **criterio minimalista**; b) el **criterio específico de la tecnología**; y c) el **criterio de doble nivel**[4].

1. Criterio minimalista

6. Algunos ordenamientos reconocen todas las tecnologías de firma electrónica, adoptando una política de neutralidad tecnológica[5]. Este criterio se denomina también minimalista, pues otorga una condición jurídica mínima a todas las formas de firma electrónica. Según el criterio minimalista, se considera que las firmas electrónicas son el equivalente funcional de las firmas manuscritas, siempre que la tecnología empleada tenga la finalidad de desempeñar determinadas funciones específicas y cumpla además determinados requisitos de fiabilidad neutrales con respecto a la tecnología.

---

[3] Véase un análisis de las cuestiones que se suelen abordar en los acuerdos entre socios comerciales en Amelia H. Boss, “Electronic data interchange agreements: private contracting toward a global environment”, *Northwestern Journal of International Law and Business*, vol. 13, Nº 1 (1992), pág. 45.

[4] Susanna F. Fischer, “Saving Rosencrantz and Guildenstern in a virtual world? A comparative look at recent global electronic signature legislation,” *Journal of Science and Technology Law*, vol. 7, Nº 2 (2001), págs. 234 y sigs.

[5] Por ejemplo, Australia y Nueva Zelandia.

7. La Ley Modelo de la CNUDMI sobre Comercio Electrónico[6] prevé lo que es el conjunto de criterios legislativos de uso más extendido para establecer una equivalencia funcional genérica entre las firmas electrónicas y las manuscritas. El párrafo 1 del artículo 7 de la Ley Modelo dispone lo siguiente:

> "1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:
>
> a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y
>
> b) si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente."

8. Esta disposición contempla las dos funciones principales de las firmas manuscritas, es decir, identificar al firmante, e indicar la intención del firmante respecto de la información firmada. Según la Ley Modelo sobre Comercio Electrónico, debe considerarse que cualquier tecnología que pueda suministrar esas dos funciones en forma electrónica satisface el requisito legal de firma. Así pues, la Ley Modelo es neutral respecto de la tecnología; es decir, no depende de la utilización de ningún tipo concreto de tecnología, ni lo presupone, y podría aplicarse a la comunicación y el almacenaje de todo tipo de información. La neutralidad tecnológica reviste particular importancia habida cuenta de la rapidez de la innovación tecnológica y contribuye a garantizar que la legislación siga pudiendo dar cabida a las novedades futuras y no resulte anticuada muy pronto. En consecuencia, la Ley Modelo evita cuidadosamente toda referencia a métodos técnicos concretos de transmisión o almacenaje de información.

9. Este principio general ha sido incorporado a la legislación de numerosos países. El principio de la neutralidad tecnológica también permite dar cabida a innovaciones tecnológicas futuras. Además, este criterio destaca la libertad de las partes de elegir tecnología que se ajuste a sus necesidades. Se hace pues hincapié en la capacidad de las partes de determinar el nivel de seguridad que resulte idóneo para sus comunicaciones. Con ello se podrá evitar una complejidad tecnológica excesiva y los costos que conlleva[7].

---

[6] Véase la nota [...] [publicación de las Naciones Unidas, Nº de venta S.99.V.4].

[7] S. Mason, "Electronic signatures in practice", *Journal of High Technology Law,* vol. VI, Nº 2 (2006), pág. 153.

10. Con la excepción de Europa, cuya legislación se ha visto influida principalmente por las directivas promulgadas por la Unión Europea[8], casi todos los países que han promulgado legislación relacionada con el comercio electrónico se han servido de la Ley Modelo sobre Comercio Electrónico como plantilla[9]. La Ley Modelo también ha servido de base para la armonización interna de la legislación sobre comercio electrónico en países organizados con carácter federal, como el Canadá[10] y los Estados Unidos de América[11]. Con poquísimas excepciones[12], los

---

[8] En particular, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica (véase la nota [...]) [*Diario Oficial de las Comunidades Europeas*, L 13]. A la Directiva sobre la firma electrónica siguió otra de carácter más general, la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (*Diario Oficial de las Comunidades Europeas*, L 178, 17 de julio de 2000), que se ocupa de varios aspectos de la prestación de servicios de tecnología de la información y algunos asuntos de la contratación electrónica.

[9] A enero de 2007, se había adoptado legislación dando aplicación a disposiciones de la Ley Modelo de la CNUDMI sobre Comercio Electrónico al menos en los siguientes países: Australia, Ley de operaciones electrónicas, 1999; China, Ley de firmas electrónicas, promulgada en 2004; Colombia, Ley de comercio electrónico; Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos (2002); Eslovenia, Ley de comercio electrónico y firma electrónica (2000); Filipinas, Ley de comercio electrónico (2000); Francia, *Loi 2000-230 portant adaptation du droit de la preuve aux technologies de l´information et relative à la signature électronique (2000)*; India, Ley de tecnología de la información, 2000; Irlanda, Ley de comercio electrónico, 2000; Jordania, Ley de operaciones electrónicas, 2001; Mauricio, Ley de operaciones electrónicas, 2000; México, Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de protección al consumidor (2000); Nueva Zelandia, Ley de operaciones electrónicas, 2002; Pakistán, Ordenanza de operaciones electrónicas, 2002; Panamá, Ley de firma digital (2001); República de Corea, Ley Marco de comercio electrónico (2001); República Dominicana, Ley sobre comercio electrónico, documentos y firmas digitales (2002); Singapur, Ley de operaciones electrónicas (1998); Sri Lanka, Ley de operaciones electrónicas (2006); Sudáfrica, Ley de comunicaciones y operaciones electrónicas (2002); Tailandia, Ley de operaciones electrónicas (2001); Venezuela (República Bolivariana de), Ley sobre mensajes de datos y firmas electrónicas (2001); y Viet Nam, Ley de operaciones electrónicas (2006). La Ley Modelo ha sido adoptada también en las dependencias de la Corona británica de la Bailía de Guernsey (Ley de operaciones electrónicas (Guernsey), 2000), la Bailía de Jersey (Ley de comunicaciones electrónicas (Jersey), 2000) y la Isla de Man (Ley de operaciones electrónicas, 2000); en los territorios de ultramar del Reino Unido de Gran Bretaña e Irlanda del Norte de las Bermudas (Ley de operaciones electrónicas, 1999), las Islas Caimán (Ley de operaciones electrónicas, 2000) y las Islas Turcas y Caicos (Ordenanza de operaciones electrónicas, 2000); y en la región Administrativa Especial (RAE) de Hong Kong (China) (Ordenanza de operaciones electrónicas (2000)). Salvo que se indique lo contrario, las referencias que se hagan a partir de ahora a disposiciones legales de cualquiera de estos países se remiten a disposiciones que figuran en las normas legislativas enumeradas *supra*.

[10] La incorporación al derecho interno de la Ley Modelo en el Canadá es la Ley Uniforme de comercio electrónico, aprobada por la Conferencia de Derecho Uniforme del Canadá en 1999 (disponible con comentario oficial en http://www.chlc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia, consultada el 12 de abril de 2007). La Ley ha sido promulgada en una serie de provincias y territorios del Canadá, a saber, Alberta, Columbia Británica, Isla del Príncipe Eduardo, Manitoba, Nueva Brunswick, Nueva Escocia, Ontario, Saskatchewan, Terranova y Labrador y Yukón. La Provincia de Québec promulgó legislación específica (la Ley por la que se establece un marco jurídico para la

países que han incorporado la Ley Modelo han conservado su criterio neutral respecto de la tecnología y no han prescrito ni favorecido la utilización de ninguna tecnología en concreto. Tanto la Ley Modelo de la CNUDMI sobre Firmas Electrónicas[13], que fue aprobada en 2001, y la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales[14], más reciente (que fue aprobada por la Asamblea General el 23 de noviembre de 2005 y ha quedado abierta a la firma desde el 16 de enero de 2006) adopta el mismo criterio, aunque la Ley Modelo de la CNUDMI sobre Firmas Electrónicas contiene texto suplementario (véase *infra*, párrs. [...] a [...]).

11. Cuando la legislación adopta el criterio minimalista, normalmente corresponde a un juez, árbitro o autoridad pública determinar la cuestión de si se ha demostrado la equivalencia de la firma electrónica, generalmente por medio de la denominada "prueba de la fiabilidad apropiada". Con arreglo a esta prueba, todos los tipos de firma electrónica que la superen se consideran válidos; así pues, la prueba consagra el principio de la neutralidad tecnológica.

12. A la hora de determinar si, atendidas todas las circunstancias del caso, un método concreto de autenticación ofrece un nivel de fiabilidad apropiado, se podrá tomar en cuenta toda una serie de factores jurídicos, técnicos y comerciales, como los siguientes: a) el grado de complejidad técnica del equipo utilizado por cada una de las partes; b) la naturaleza de su actividad comercial; c) la frecuencia con la que tienen lugar operaciones comerciales entre las partes; d) la naturaleza de la operación y su envergadura; e) la función de los requisitos de firma en un determinado ordenamiento legal y reglamentario; f) la capacidad de los sistemas de comunicación; g) el cumplimiento de los procedimientos de autenticación

---

tecnología de la información (2001)), que, aunque tiene un alcance más amplio y está redactada de forma muy diferente, cumple muchos de los objetivos de la Ley Uniforme de Comercio Electrónico y es por lo general compatible con la Ley Modelo de la CNUDMI sobre Comercio Electrónico. En http://www.chlc.ca/en/cls/index.cfm?sec=4&sub=4b>, puede obtenerse información actualizada sobre la promulgación de la Ley Uniforme de Comercio Electrónico, consultada el 7 de febrero de 2007.

[11] En los Estados Unidos de América, la Conferencia Nacional de Comisarios de Leyes Uniformes de los Estados se sirvió de la Ley Modelo de la CNUDMI sobre Comercio Electrónico como base para preparar la Ley Uniforme de operaciones electrónicas, que adoptó en 1999 (el texto de la Ley y el comentario oficial están disponibles en http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm, consultados el 7 de febrero de 2007). La Ley Uniforme de operaciones electrónicas ha sido incorporada al derecho interno en el Distrito de Columbia y en los 46 Estados siguientes: Alabama, Alaska, Arizona, Arkansas, California, Carolina del Norte, Carolina del Sur, Colorado, Connecticut, Dakota del Norte, Dakota del Sur, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Luisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, Nueva Jersey, Nuevo Hampshire, Nuevo México, Ohio, Oklahoma, Oregón, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Virginia, Virginia Occidental, Wisconsin y Wyoming. Es probable que otros Estados adopten legislación de aplicación en un futuro próximo, incluido el Estado de Illinois, que ya había incorporado a su derecho interno la Ley Modelo de la CNUDMI mediante la Ley de seguridad del comercio electrónico (1998). Puede encontrarse información actualizada sobre la incorporación de la Ley Uniforme de operaciones electrónicas en http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp, consultada el 7 de febrero de 2007.

[12] Colombia, Ecuador, India, Mauricio, Panamá, República Dominicana y Sudáfrica.

[13] Véase la nota [...] [publicación de las Naciones Unidas, Nº de venta S.02.V.8].

[14] Véase la nota [...] [resolución 60/21 de la Asamblea General, anexo].

establecidos por los intermediarios; h) la gama de procedimientos de autenticación facilitados por cualquier intermediario; i) el cumplimiento de los usos y prácticas del comercio; j) la existencia de mecanismos de cobertura de seguros contra mensajes no autorizados; k) la importancia y el valor de la información consignada en el mensaje de datos; l) la existencia de otros métodos de identificación y el costo de su aplicación; y m) el grado de aceptación y de no aceptación del método de identificación en la industria o esfera pertinentes tanto en el momento en que el método fue convenido como en el momento en que el mensaje de datos fue comunicado.

2. Criterio de la tecnología específica

13. La preocupación de promover la neutralidad respecto de los medios plantea otras cuestiones importantes. La imposibilidad de garantizar una seguridad absoluta contra el fraude y el error de transmisión no se limita al mundo del comercio electrónico, sino que es igualmente aplicable al mundo de los documentos de papel. Al formular normas sobre el comercio electrónico, los legisladores suelen inclinarse a conseguir el máximo nivel de seguridad que ofrece la tecnología existente[15]. No cabe poner en duda la necesidad práctica de aplicar medidas de seguridad estrictas para evitar el acceso no autorizado a los datos, garantizar la integridad de las comunicaciones y proteger los sistemas informáticos. Ahora bien, desde la perspectiva del derecho mercantil privado, tal vez sea más idóneo clasificar los requisitos de seguridad en grados similares a los grados de seguridad jurídica que existen en el mundo de papel. En este último mundo, los comerciantes pueden elegir, en la mayoría de los casos, entre una amplia gama de métodos para conseguir la integridad y la autenticidad de las comunicaciones (por ejemplo, los distintos niveles de firma manuscrita que se ven en documentos de contratos sencillos y actos protocolizados notarialmente). En el marco de un criterio de tecnología específica, la normativa obligaría a que una tecnología específica cumpliera los requisitos legales para la validez de una firma electrónica. Así ocurre, por ejemplo, cuando la ley, pretendiendo alcanzar un nivel más alto de seguridad, exige aplicaciones basadas en infraestructuras de clave pública (ICP). Como prescribe la utilización de una tecnología específica, se denomina también el criterio “prescriptivo”.

---

[15] Uno de los primeros ejemplos fue la Ley de firma digital de Utah, que fue aprobada en 1995, pero derogada a partir del 1º de mayo de 2006 por el proyecto de ley estatal 20, disponible en http://www.le.state.ut.us/~2006/htmdoc/sbillhtm/sb0020.htm, consultado el 28 de marzo de 2007. El sesgo tecnológico de la Ley de Utah puede observarse también en cierto número de países en los que la ley únicamente reconoce las firmas digitales creadas en el marco de una infraestructura de clave pública (ICP) como medio válido de autenticación electrónica, lo que ocurre por ejemplo en las leyes de: Alemania, Ley de firma digital, promulgada como artículo 3 de la Ley de servicios de información y comunicación de 13 de junio de 1997; Argentina, Ley de firma digital (2001) y Decreto Nº 2628/2002 (Reglamentación de la Ley de firma digital); Estonia, Ley de firmas digitales (2000); Federación de Rusia, Ley sobre la firma digital electrónica (2002); India, Ley de tecnología de la información, 2000; Israel, Ley de firma electrónica (2001); Japón, Ley relativa a firmas electrónicas y servicios de certificación (2001); Lituania, Ley sobre firmas electrónicas (2000); Malasia, Ley de firma digital, 1997; y Polonia, Ley sobre firma electrónica (2001).

14. El criterio de la tecnología específica tiene las desventajas de que, al favorecer tipos específicos de firma electrónica, "corre el riesgo de impedir que otras tecnologías posiblemente superiores entren y compitan en el mercado"[16]. En lugar de facilitar el crecimiento del comercio electrónico y la utilización de técnicas de autenticación electrónica, ese criterio puede surtir el efecto contrario. La legislación de tecnología específica corre el riesgo de establecer requisitos antes de que una tecnología concreta se consolide[17]. En ese caso, es posible que la legislación impida la evolución positiva posterior de la tecnología o que quede anticuada rápidamente como consecuencia de posteriores innovaciones. Otro aspecto es que tal vez no sea necesario para todas las aplicaciones un nivel de seguridad comparable que ofrecen determinadas técnicas específicas, como las firmas digitales. También puede darse el caso de que la rapidez y la facilidad de comunicación u otros aspectos puedan resultar más importantes para las partes que garantizar la integridad de la información electrónica mediante cualquier proceso concreto. Al exigir la utilización de medios de autenticación excesivamente seguros se podría ocasionar el despilfarro de costos y de esfuerzos, lo que tal vez obstaculice la difusión del comercio electrónico.

15. La legislación de la tecnología específica favorece la utilización de firmas digitales en el marco de una ICP. A su vez, la forma en que estas ICP están estructuradas es distinta de un país a otro según el nivel de intervención estatal. En esta esfera, también pueden señalarse tres modelos principales:

a) **Autorreglamentación**. Según este modelo, el terreno de la autenticación queda abierto de par en par. Aunque el gobierno pueda establecer un sistema de autenticación o más en sus propios departamentos y organizaciones conexas, el sector privado puede establecer los planes de autenticación, de carácter comercial o de otra índole, que estime pertinente. No existe una alta autoridad de autenticación de carácter imperativo y los prestadores de servicios de autenticación son responsables de garantizar la interoperabilidad con otros prestadores, nacionales e internacionales, según los objetivos que se persigan con el establecimiento del sistema de autenticación. Las licencias o aprobaciones de la tecnología de los prestadores de servicios de autenticación no son obligatorias (con la posible excepción de la normativa de protección del consumidor)[18];

b) **Intervención estatal limitada**. El gobierno puede decidir establecer una alta autoridad de autenticación de carácter voluntario o imperativo. En este caso, los prestadores de servicios de autenticación tal vez se vean obligados a interoperar con la alta autoridad de autenticación para que sus símbolos de autenticación (u otros medios de autenticación) sean aceptados fuera de sus propios sistemas. En este caso,

---

[16] Stewart Baker y Matthew Yeo, en colaboración con la secretaría de la Unión Internacional de Telecomunicaciones "*Background and Issues Concerning Authentication and the ITU*", documento informativo presentado a la reunión de expertos en firmas electrónicas y autoridades de certificación: cuestiones relacionadas con las telecomunicaciones, Ginebra, 9 y 10 de diciembre de 1999, documento Nº 2, disponible en http://www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html, consultado el 12 de abril de 2007.

[17] No obstante, habida cuenta del hecho de que la ICP está ya bastante consolidada y establecida, puede que algunas de estas preocupaciones no tengan ya el mismo peso.

[18] Foro de Cooperación de Asia y el Pacífico, *Assessment Report on Paperless Trading of APEC Economies* (Beijing, secretaría del APEC, 2005), págs. 63 y 64, en las que se cita a los Estados Unidos como ejemplo de la aplicación de este modelo.

deben publicarse lo antes posible las especificaciones técnicas y de gestión de los prestadores de servicios de autenticación para que los departamentos estatales y el sector privado puedan formular sus correspondientes planes. Podrían exigirse licencias y aprobaciones de tecnología en el caso de cada prestador de servicios de autenticación[19];

c) **Proceso dirigido por el gobierno**. El gobierno podrá decidir establecer un prestador de servicios de autenticación central exclusivo. También se podrán establecer prestadores de servicios de autenticación especiales con autorización del gobierno[20]. Los sistemas de gestión de la identidad (véanse los párrs. [...] a [...] *supra*) constituyen otra forma en la que los gobiernos podrán dirigir indirectamente el proceso de firma digital. Algunos gobiernos ya han puesto en marcha programas para expedir a sus ciudadanos documentos de identidad legibles por máquina ("identificaciones electrónicas") dotados de funcionalidades de firma digital.

3. Criterio de doble nivel

16. Según este criterio, la legislación establece un umbral bajo de requisitos para que los métodos de autenticación electrónica reciban un determinado estatuto jurídico mínimo y asigna mayor efecto jurídico a determinados métodos de autenticación electrónica (a los que se denomina de diversas formas firmas electrónicas seguras, avanzadas o refrendadas, o certificados reconocidos)[21]. En el plano básico, la legislación que adopta un sistema de doble nivel suele otorgar a las firmas electrónicas la equivalencia funcional con las firmas manuscritas, sobre la base de criterios neutrales respecto de la tecnología. Las firmas de más alto nivel, a las que son aplicables determinadas presunciones *juris tantum*, deben cumplir requisitos específicos que pueden guardar relación con una tecnología concreta. En la actualidad, la legislación de este tipo suele definir dichas firmas seguras en términos de tecnología de IFP.

17. Suele optarse por este criterio en foros en los que se considera importante abordar determinados requisitos tecnológicos en su legislación pero que, al mismo tiempo, desean dejar margen para las innovaciones tecnológicas. Este criterio puede aportar equilibrio entre la flexibilidad y la certidumbre en relación con las firmas electrónicas al dejar que las partes decidan, como criterio comercial, si el costo y la inconveniencia de utilizar un método más seguro se ajusta a sus necesidades. Dichos textos también facilitan orientación sobre los criterios para el reconocimiento de firmas electrónicas en el contexto de un modelo de autoridad de certificación. Por lo general se puede combinar el criterio de doble nivel con cualquier tipo de modelo de certificación (ya sea un sistema autorreglamentado, de acreditación voluntaria o dirigido por el gobierno), de forma muy parecida a lo que podría hacerse en el marco del criterio de la tecnología específica (véase *supra*, párr. [...] a [...]). Así pues, si bien es cierto que algunas normas pueden tener suficiente flexibilidad para dar cabida a distintos modelos de certificación de la firma electrónica, algunos sistemas reconocerían únicamente a los prestadores de servicios de certificación autorizados como posibles emisores de certificados "seguros" o "reconocidos".

---

[19] Ibíd., donde se cita como ejemplo a Singapur.

[20] Ibíd., donde se cita como ejemplos a China y Malasia.

[21] Aalberts y van der Hof, *Digital Signature Blindness* ... (véase la nota [...]), párr. 3.2.2.

18. Entre los primeros foros que han aprobado legislación por la que se adopta el criterio de doble nivel figuran Singapur[22] y la Unión Europea[23]. Les siguieron otros ordenamientos jurídicos[24]. La Ley Modelo de la CNUDMI sobre Firmas Electrónicas autoriza al Estado promulgante a establecer un sistema de doble nivel mediante la reglamentación pertinente, aunque no lo promueve activamente[25].

19. En cuanto al segundo nivel, se propuso que los países no exigieran la utilización de firmas de segundo nivel como requisito de forma en relación con operaciones comerciales internacionales y que las firmas electrónicas "seguras" se limitaran a ámbitos del derecho que no tengan repercusiones importantes en el comercio internacional (por ejemplo, fideicomisos, derecho de familia, operaciones inmobiliarias, etc.)[26]. Además, se sugirió que la legislación de doble nivel diera

---

[22] El artículo 8 de la Ley de operaciones electrónicas de Singapur admite cualquier forma de firma electrónica, pero únicamente las firmas electrónicas seguras que cumplan los requisitos del artículo 17 de la Ley (es decir, las que son "a) exclusivas de la persona que las utiliza; b) permiten identificar a esa persona; c) creadas de manera o utilizando medios bajo el control exclusivo de la persona que las utiliza; y d) vinculadas al registro electrónico con el que guardan relación de manera que si el registro se alterara la firma electrónica perdería su validez") se pueden acoger a las presunciones enumeradas en el artículo 18 (entre otras cosas, que la firma "es de la persona con la que está relacionada" y que la firma "fue estampada por esa persona con la intención de firmar o aprobar el registro electrónico"). Las firmas electrónicas respaldadas por un certificado fiable que cumpla lo dispuesto en el artículo 20 de la Ley se consideran automáticamente "firmas electrónicas seguras" a los efectos de la Ley.

[23] Al igual que la Ley de operaciones electrónicas de Singapur, la Directiva de la Unión Europea sobre la firma electrónica (véase la nota [...]), distingue entre una "firma electrónica" (que se define en el párr. 1 del artículo 2 como "los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como método de autenticación") y una "firma electrónica avanzada" (que se define en el párr. 2 del art. 2 como una firma electrónica que cumple los requisitos siguientes: "a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada, utilizando medios que el firmante puede mantener bajo su exclusivo control; y d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable"). En el párrafo 2 de su artículo 5, la Directiva encomienda a los Estados miembros de la Unión Europea que velen por que "no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho de que ésta se presente en forma electrónica, o no se base en un certificado reconocido, o no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o no esté creada por un dispositivo seguro de creación de firma". No obstante, se declara que únicamente la firma electrónica avanzada "basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma" satisface "[...] el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel; y b) [es] admisible como prueba en procedimientos judiciales". (véase el párr. 1 del art. 5 de la Directiva.)

[24] Por ejemplo, Mauricio y el Pakistán. Véanse detalles de las respectivas normas legislativas en la nota [9] *supra*.

[25] La Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase la nota [...]), en el párrafo 3 de su artículo 6, dispone que la firma electrónica se considerará fiable 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.

[26] Baker y Yeo, "Background and issues concerning authentication ..." (véase la nota [16]).

efectividad explícitamente a los acuerdos contractuales relativos a la utilización y el reconocimiento de firmas electrónicas, a fin de garantizar que los modelos mundiales de autenticación basados en contratos no vulneren las prescripciones legales internas.

B. Valor probatorio de los métodos de firma y autenticación electrónicas

20. Uno de los objetivos principales de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y la Ley Modelo de la CNUDMI sobre Firmas Electrónicas consistía en prevenir la falta de armonía y el posible exceso de reglamentación al ofrecer para ello criterios generales para establecer la equivalencia funcional entre métodos de firma y autenticación electrónicas y basadas en papel. Aunque la Ley Modelo de la CNUDMI sobre Comercio Electrónico ha tenido mucha aceptación, y un creciente número de Estados se han servido de ella como base para su legislación sobre comercio electrónico, no cabe suponer todavía que los principios de la Ley Modelo hayan alcanzado una aplicación universal. La actitud adoptada por diversos foros en relación con la firma y la autenticación electrónicas suele reflejar el criterio general del foro correspondiente en relación con los requisitos de escritura y el valor probatorio de registros electrónicos.

1. “Autenticación” y asignabilidad general de los registros electrónicos

21. En la utilización de métodos de autenticación electrónica hay dos aspectos de interés para el presente examen. El primero es la cuestión general de la asignabilidad de un mensaje a su supuesto iniciador. El segundo es la idoneidad del método de identificación utilizado por las partes para cumplir determinados requisitos de forma, en particular los requisitos legales de firma. También son importantes los conceptos jurídicos en que se presuponga la existencia de la firma manuscrita, como el de “documento” que se utiliza en algunos ordenamientos jurídicos. Aunque estos dos aspectos pueden con frecuencia subsumirse o, según el caso, no resultar del todo diferentes, tal vez sea útil analizarlos por separado, porque al parecer los tribunales tienden a sacar conclusiones diferentes según la función que se asigne al método de autenticación.

22. La Ley Modelo de la CNUDMI sobre Comercio Electrónico se refiere en su artículo 13 a la atribución de los mensajes de datos. Esta disposición se origina en el artículo 5 de la Ley Modelo de la CNUDMI sobre Transferencias Internacionales de Crédito[27], en que se definen las obligaciones del expedidor de una orden de pago. La aplicación del artículo 13 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico se prevé para los casos en que haya dudas respecto de si una determinada comunicación electrónica fue enviada realmente por la persona a la que se indica como el “iniciador”. En el caso de una comunicación basada en papel, el problema se plantearía si se tratara de la firma presuntamente falsificada del supuesto “iniciador”. En un entorno electrónico, el remitente del mensaje podría ser una persona sin autorización, pero su autenticación mediante código, cifrado o medios análogos sería correcta. El objetivo del artículo 13 no es asignar la autoría

[27] Publicación de las Naciones Unidas, Nº de venta S.99.V.11, que puede consultarse en http://www.uncitral.org/pdf/spanish/texts/payments/transfers/ml-credittranss.pdf.

de un mensaje de datos ni establecer la identidad de las partes. Se refiere más bien a la asignabilidad o atribución de los mensajes de datos, estableciendo las condiciones en que una parte puede dar por sentado que un determinado mensaje de datos provenía efectivamente del supuesto iniciador.

23. En el párrafo 1 del artículo 13 de la Ley Modelo sobre Comercio Electrónico se recuerda el principio de que el iniciador queda vinculado a un mensaje de datos si ha enviado efectivamente dicho mensaje. El párrafo 2 se refiere a la situación en que haya enviado el mensaje una persona que no fuera el iniciador pero facultada para actuar en su nombre. El párrafo 3 se refiere a dos situaciones en que el destinatario podría confiar en que el mensaje de datos proviene del iniciador: en primer lugar, aquélla en que el destinatario haya aplicado adecuadamente un procedimiento de autenticación aceptado previamente por el iniciador; y, en segundo, las situaciones en que el mensaje de datos resulte de los actos de una persona cuya relación con el iniciador, le haya dado acceso a los procedimientos de autenticación de dicho iniciador.

24. Varios países han adoptado la norma del artículo 13 de la Ley Modelo sobre Comercio Electrónico, incluida la presunción de autoría establecida en el párrafo 3 de dicho artículo[28]. Algunos países se refieren expresamente a la utilización de códigos, contraseñas u otros medios de identificación como factores que crean la presunción de autoría[29]. Existen también versiones más generales del artículo 13, en que la presunción basada en una verificación correcta mediante un procedimiento convenido con anterioridad pasa a considerarse indicio de elementos que pueden utilizarse a efectos de asignabilidad[30].

25. Sin embargo, otros países han adoptado únicamente las normas generales del artículo 13, concretamente las que establecen que el mensaje de datos es el del iniciador si lo envió éste o una persona que actuara en su nombre, o si se envió mediante un sistema programado para funcionar automáticamente por el iniciador o en su nombre[31]. Además, varios países que han aplicado la Ley Modelo sobre Comercio Electrónico no han incorporado disposiciones concretas basadas en su

---

[28] Colombia (art. 17); Ecuador (art. 10); Filipinas (art.. 18, párr. 3); Jordania (art. 15); Mauricio (art. 12, párr. 2); República de Corea (art. 7, párr. 2); Singapur (art. 13, párr. 3); Tailandia (art. 16); y Venezuela (República Bolivariana de) (art. 9). Las mismas normas figuran en las leyes de la dependencia de la Corona británica de Jersey (art. 8) y en los territorios británicos de ultramar de las Bermudas (art. 16, párr. 2) y Turcas y Caicos (art. 14). Los pormenores de las leyes respectivas figuran en la nota [9] *supra*.

[29] México (véase la nota [9] *supra*), art. 90, párr. I.

[30] Por ejemplo, la Ley Uniforme de operaciones electrónicas de los Estados Unidos (véase la nota [10]) dispone, en el párrafo a) del artículo 9, que un documento o una firma electrónicos "podrá atribuirse a una persona si es resultado del acto de dicha persona. El acto de la persona podrá demostrarse de cualquier forma, por ejemplo demostrando la eficacia de todo procedimiento de seguridad utilizado para determinar la persona a la que pueda atribuirse el registro o la firma electrónicos. "En el párrafo b) del artículo 9 se dispone, además, que el efecto de un registro o firma electrónicos atribuidos a una persona con arreglo a lo dispuesto en el párrafo a)" se determina según el contexto y las circunstancias de su creación, ejecución o aprobación, incluido el acuerdo de las partes, de haberlo, y de cualquier otra forma prevista en la legislación."

[31] Australia (art. 15, párr. 1); en lo esencial del mismo modo, Eslovenia (art. 5); la India (art. 11); el Pakistán (art.13, párrafo 2); la dependencia de la Corona británica de la Isla de Man (art. 2); la Región Administrativa Especial de Hong Kong (China) (art. 18). Los pormenores de las leyes respectivas figuran en la nota [9], *supra*.

artículo 13[32]. En estos países se daba por supuesto que no se requerían normas concretas y que lo mejor era utilizar los métodos comunes de prueba para asignar el mensaje, como era el caso de la asignación de los documentos en papel: "La persona que desee confiar en una firma corre el riesgo de que ésta sea inválida, y esta norma no se modifica en el caso de las firmas electrónicas"[33].

26. Sin embargo, otros países han preferido separar las disposiciones de la Ley Modelo sobre Comercio Electrónico relativas a la asignación de las relativas a la firma electrónica. Ello se basa en el entendimiento de que la asignabilidad en el caso de los documentos cumple la función primordial de establecer una base de confianza razonable, y puede incluir más medios que los utilizados estrictamente para identificar a personas. En algunas leyes, como la Ley Uniforme de operaciones electrónicas de los Estados Unidos, se subraya este principio señalando, por ejemplo, que "un registro o firma electrónicos podrá atribuirse a una persona si es resultado del acto de dicha persona", lo que "podrá demostrarse de cualquier forma, por ejemplo, demostrando la eficacia de todo procedimiento de seguridad utilizado para determinar la persona a la que pueda atribuirse el registro o la firma electrónicos"[34]. Esta norma general sobre asignabilidad no incide en la utilización de la firma como mecanismo para asignar el registro a determinada persona, sino que se basa en el reconocimiento de que "la firma no es el único método de atribución"[35]. Por ello, según el comentario sobre la Ley de los Estados Unidos:

> "4. Es posible que en un contexto electrónico consten ciertos datos que, aunque no lo parezca, permitan atribuir claramente determinado documento a determinada persona. Elementos como los códigos digitales, los números de identificación personal y las combinaciones de claves públicas y privadas sirven para determinar la persona a la que haya de atribuirse un documento electrónico. Naturalmente, los procedimientos de seguridad constituyen otra

---

[32] Por ejemplo, el Canadá, Francia, Irlanda, Nueva Zelandia y Sudáfrica.

[33] Canadá, Ley Uniforme de comercio electrónico (con comentario oficial) (véase la nota [10]), comentario del artículo 10.

[34] Estados Unidos, Ley Uniforme de operaciones electrónicas (1999) (véase la nota [11]), artículo 9. En el párrafo 1 de los comentarios oficiales sobre el artículo 9 se presentan los ejemplos siguientes, en que el registro y la firma electrónicos podrían atribuirse a una determinada persona: el caso en que una persona "mecanografía su nombre en un pedido de compra por correo electrónico"; aquél en que el "empleado de una persona, facultado para ello, mecanografía el nombre de dicha persona en un pedido de compra por correo electrónico"; o el caso en que "la computadora de una persona, programada para pedir mercancías tras recibir información de inventario conforme a determinados parámetros, expide un pedido de compra en que figure el nombre de la persona u otra información de identificación como parte del pedido".

[35] Ibíd. El párrafo 3 de los comentarios oficiales sobre el artículo 9 señala que "las transmisiones por facsímil suministran diversos ejemplos de atribución mediante información distinta de la firma. Un fax puede atribuirse a una determinada persona por la información impresa en la parte superior de la página en que se indica la máquina desde la que se envió. De manera análoga, la trasmisión puede llevar un membrete en que se identifique al remitente. En algunos casos judiciales se ha considerado que este membrete constituía efectivamente una firma, por ser el símbolo adoptado por el remitente para autentificar el facsímil. Sin embargo, la determinación de la autoría de la firma se basaba en la necesaria determinación de la intención en dicho caso. En otros fallos se ha dictaminado que el membrete del fax NO constituía firma porque no existía la intención necesaria. El aspecto determinante es que, con o sin firma, la información consignada en el registro electrónico puede bastar para asignar el registro electrónico a una parte determinada.".

modalidad de prueba con la que puede determinarse la autoría de un documento.

Toda referencia expresa a los procedimientos de seguridad como medio de probar la autoría es útil por la importancia singular de esos procedimientos en el ámbito electrónico. En determinadas causas, el dispositivo de seguridad técnico utilizado tal vez sea el argumento más eficaz para obtener un dictamen pericial de los hechos que confirme que cabe atribuir una determinada firma o documento electrónico a determinada persona. En ciertas circunstancias, la utilización de un procedimiento de seguridad que permita determinar que un documento y su firma proceden del negocio de determinada persona puede ser un factor decisivo para contrarrestar alguna pretensión falsa de que ha intervenido en la operación un pirata informático. Esta insistencia en los procedimientos de seguridad no quisiera sugerir que deban asignarse efectos menos convincentes a otras formas probatorias de la autoría. Conviene también recordar que la ventaja intrínseca de un determinado procedimiento no depende tanto de su condición de procedimiento de seguridad como del valor probatorio que se le asigne a dicho procedimiento de seguridad como elemento para determinar la autoría[36]."

27. También cabe tener presente que la presunción de autoría por sí sola no restaría validez a las normas legales sobre la firma, en los casos en que ésta se requiera para dar validez o probar un acto. Una vez establecido que una firma o documento es atribuible a una parte determinada, "el efecto de una firma o documento deberá ser determinado en función del contexto y las circunstancias, así como de todo acuerdo entre las partes, si lo hubiere", y de "cualquier otro requisito legal que se prevea según el contexto"[37].

28. Con el trasfondo de este concepto flexible de la autoría, al parecer los tribunales de los Estados Unidos han adoptado un criterio abierto respecto de la admisibilidad de los registros electrónicos, incluido el correo electrónico, como pruebas en actuaciones civiles[38]. Los tribunales de los Estados Unidos han desestimado los argumentos en el sentido de que los mensajes de correo electrónico son inadmisibles como prueba porque se trata de testimonios verbales no autenticados[39]. Los tribunales han dictaminado en cambio que los correos electrónicos del demandante durante el trámite de proposición de prueba se autenticaban por sí solos, porque "la presentación de documentos tomados de los archivos de las partes durante dicho trámite de proposición de prueba basta para

---

[36] Ibíd., comentario oficial sobre el artículo 9.

[37] Ibíd., párrafo 6 de los comentarios oficiales sobre el artículo 9.

[38] *Commonwealth Aluminum Corporation* contra *Stanley Metal Associates*, Tribunal de distrito de los Estados Unidos del distrito occidental de Kentucky, 9 de agosto de 2001, *Federal Supplement, 2nd series*, vol. 186, pág. 770; y *Central Illinois Light Company (CILCO)* contra *Consolidation Coal Company (Consol)*, Tribunal de distrito de los Estados Unidos del distrito central de Illinois, 30 de diciembre de 2002, *Federal Supplement, 2nd series*, vol. 285, pág. 916.

[39] *Sea-Land Service, Inc.* contra *Lozen International, LLC*, Tribunal de Apelaciones de los Estados Unidos, noveno circuito, 3 de abril de 2002, *Federal Reporter, 3rd series*, vol. 285, pág. 808.

justificar un dictamen de autoautenticación"[40]. Los tribunales tienden a tener en cuenta todas las pruebas existentes y no rechazan la documentación electrónica por razón de presunta inadmisibilidad.

29. En los países que no han adoptado la Ley Modelo sobre Comercio Electrónico no existen al parecer normas sobre mecanismos de atribución análogos. En ellos, la asignación de autoría depende característicamente del reconocimiento legal de la firma electrónica y de las presunciones relativas a los documentos autenticados con determinados tipos de firma electrónica. Por ejemplo, las inquietudes sobre el riesgo de manipulación de los documentos electrónicos han determinado que los tribunales de estos países desestimen el valor probatorio de los correos electrónicos en las actuaciones judiciales, aduciendo que no garantizan suficientemente la integridad[41]. Otros ejemplos de un enfoque restrictivo del valor probatorio de los documentos electrónicos y la asignación de autoría se observan en casos recientes relativos a subastas por Internet, en que los tribunales han aplicado una norma exigente para la asignación de la autoría de los mensajes de datos. Se trataba con frecuencia de demandas por incumplimiento de contrato basadas en el impago de mercancías supuestamente adquiridas en subastas por Internet. En ellas, el demandante sostenía que el demandado era el comprador, porque la oferta más alta ofrecida por las mercancías se había autenticado con la contraseña del demandado en un mensaje enviado desde su dirección de correo electrónico. Los tribunales han determinado que esos elementos no bastaban para determinar categóricamente que el demandado había participado en la subasta y presentado la oferta ganadora, y han utilizado diversos argumentos para justificar dicha postura. Por ejemplo, que las contraseñas no eran fiables porque quien conociera la del demandado hubiera podido utilizar su dirección de correo electrónico desde cualquier lugar y participar en la subasta utilizando el nombre del demandado[42], riesgo que algunos tribunales consideraban "muy alto", basándose en dictámenes periciales relativos a amenazas a la seguridad de las redes de comunicaciones de Internet, en particular las que planteaban los "caballos de Troya", que podían "robar" contraseñas[43]. El oferente de bienes y servicios por un determinado medio de comunicación debía asumir el riesgo de todo uso no autorizado del dispositivo de identificación de una persona (contraseña), porque no había ninguna presunción jurídica que permitiera atribuir a dicha persona

---

[40] *Superhighway Consulting, Inc.* contra *Techwave Inc.,* Tribunal de distrito de los Estados Unidos del distrito norte de Illinois, división oriental, 16 de noviembre de 1999, *U.S. Dist. LEXIS 17910*.

[41] Alemania, *Amtsgericht* (Tribunal de distrito) Bonn, causa Nº 3 C 193/01, 25 de octubre de 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 332/2002, que figura en http://www.jurpc.de/rechtspr/20020332.htm, consultado el 11 de septiembre de 2003.

[42] Alemania, *Amtsgericht* (Tribunal de distrito), Erfurt, causa Nº 28 C 2354/01, 14 de septiembre de 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 71/2002, que figura en http://www.jurpc.de/rechtspr/20020071.htm, consultado el 25 de agosto de 2003; véase también Landesgericht (Tribunal del *Land*), Bonn, causa Nº 2 O 472/03, 19 de diciembre de 2003, *JurPC, Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 74/2004, que figura en http://www.jurpc.de/rechtspr/20040074.htm, consultado el 2 de febrero de 2007.

[43] Alemania, *Landesgericht* (Tribunal del *Land*) de Constanza, caso Nº 2 O 141/01 A, 19 de abril de 2002, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 291/2002, publicado en http://www.jurpc.de/rechtspr/20020291.htm, consultado el 25 de agosto de 2003.

los mensajes enviados por un sitio de Internet con la contraseña de acceso de dicha persona a ese sitio[44]. Si bien cabría admitir que tal presunción fuera aplicable al empleo de una "firma electrónica avanzada", de prescribirlo así la ley, no cabe imponer al titular de una mera "contraseña" el riesgo de que personas no autorizadas utilicen indebidamente su contraseña[45].

2. Posibilidad de cumplir los requisitos de firma

30. En algunos países, los tribunales han tendido a interpretar con flexibilidad los requisitos de firma. Como se indicó antes (véase la introducción, párr. […] a […]), así se ha hecho con frecuencia en algunos foros de derecho anglosajón en relación con las normas de la legislación sobre el fraude en el sentido de que algunas operaciones deben consignarse por escrito y llevar una firma para ser válidas. Los tribunales estadounidenses se han mostrado también abiertos al reconocimiento legal de la firma electrónica y han permitido que se utilice en situaciones no previstas expresamente en la norma legislativa por la que se autoriza su empleo, como la expedición de mandamientos judiciales[46]. Lo que es más importante en el contexto contractual, los tribunales también han evaluado la idoneidad de la autenticación conforme al trato establecido entre las partes en lugar de aplicar una norma estricta en todas las situaciones. De este modo, si las partes han utilizado habitualmente el correo electrónico en sus negociaciones, los tribunales han determinado que el nombre mecanografiado del iniciador de un correo electrónico cumple los requisitos legales de firma[47]. Se considera autenticación válida "el acto deliberado de una persona de mecanografiar su nombre al pie de sus mensajes y pedidos por correo electrónico"[48]. La disposición de los tribunales estadounidenses a reconocer que los correos electrónicos y los nombres mecanografiados en ellos pueden cumplir los requisitos de la forma escrita[49] se sigue de una interpretación amplia del concepto de "firma", por la que se entiende "toda inscripción realizada o reconocida por una parte con la intención directa de autenticar un escrito", de manera que, en algunos casos, "el nombre mecanografiado o en un documento o su membrete bastan para cumplir el requisito de firma"[50]. Si las partes no niegan haber

---

[44] Alemania, *Landesgericht* (Tribunal del *Land*), Bonn, causa Nº 2 O 450/00, 7 de agosto de 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 136/2002, publicado en http://www.jurpc.de/rechtspr/20020136.htm, consultado el 25 de agosto de 2003.

[45] Alemania, *Oberlandesgericht Köln* (Tribunal de apelación de Colonia), causa Nº 19 U 16/02, 6 de septiembre de 2002, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 364/2002, (publicada en http://www.jurpc.de/rechtspr/20020364.htm, consultado el 25 de agosto de 2003).

[46] Departamento de Agricultura y Servicios al Consumidor *contra Haire*, Cuarto tribunal de distrito de apelación de Florida, causas Núms. 4D02-2584 y 4D02-3315, de 15 de enero de 2003.

[47] *Cloud Corporation* contra *Hasbro, Inc.*, Tribunal de apelación de los Estados Unidos, séptimo circuito, 26 de diciembre de 2002, *Federal Reporter,* tercera serie, vol. 314, pág. 296.

[48] *Jonathan P. Shattuck* contra *David K. Klotzbach*, Tribunal superior de Massachusetts, 11 de diciembre de 2001, *2001 Mass. Super. LEXIS 642*.

[49] *Central Illinois Light Company* contra *Consolidation Coal Company*, Tribunal de distrito de los Estados Unidos, Distrito Central de Illinois, División de Peoria, 30 de diciembre de 2002, Federal Supplement, *2nd Series,* vol. 235, pág. 916.

[50] Ibíd., pág. 919: "Pueden utilizarse documentos internos como facturas y correos electrónicos para cumplir la legislación sobre fraude de Illinois [Código comercial uniforme]". Sin embargo, en este caso concreto, el tribunal dictaminó que el supuesto contrato no cumplía la ley sobre el

escrito o recibido comunicaciones por correo electrónico, se cumplirían los requisitos de firma previstos en la ley, porque los tribunales han "reconocido desde hace mucho tiempo que toda firma vinculante puede adoptar la forma de una marca o símbolo que considere correcta la parte que debe responder por ella, siempre que el autor "tenga la intención de reconocerla"[51].

31. Los tribunales del Reino Unido de Gran Bretaña e Irlanda del Norte han adoptado un criterio similar, considerando en general que la forma de la firma es menos importante que su función. De este modo, prestarían atención a la idoneidad del medio tanto para asignar el registro a una persona determinada como para indicar la intención de ésta con respecto a él. Por ello, los correos electrónicos pueden constituir "documentos", y los nombres mecanografiados en ellos "firmas"[52]. Algunos tribunales han declarado que "no dudan de que si una parte crea y envía un documento creado electrónicamente se considerará que lo ha firmado, tal y como en derecho se consideraría que había firmado la copia impresa del mismo documento", y que "el hecho de que el documento se haya creado electrónicamente y no en formato impreso no significa nada"[53]. En ocasiones, los tribunales han rechazado los argumentos en el sentido de que el correo electrónico constituía un contrato firmado a efectos de la ley de fraude, principalmente porque faltaba la intención de declararse obligado por la firma. Sin embargo, no parece haber precedentes de denegación *a priori* por el tribunal de la posibilidad de que los mensajes de correo electrónico y los nombres mecanografiados en ellos cumplan los requisitos relativos a la forma escrita y a la firma previstos en la legislación. En algunos casos, se determinó que no se cumplían los requisitos de la ley sobre fraude porque los correos electrónicos en cuestión reflejaban únicamente negociaciones en curso y no un acuerdo definitivo, por ejemplo porque durante esas negociaciones una de las partes había previsto que se celebrara un contrato vinculante únicamente después de que se firmara un "memorando de negociaciones"[54]. En otros casos, los tribunales han insinuado que podrían inclinarse a admitir como firma "el nombre o las iniciales" del iniciador "al final del correo electrónico" o "en cualquier parte del texto del mensaje", pero han considerado que "la inserción automática de la dirección de correo electrónico después de la transmisión del documento por el [prestador de servicios de Internet] remitente o destinatario" no se consideraba "firma"[55]. Aunque los tribunales británicos parecen interpretar los requisitos de forma previstos en la ley sobre fraude más estrictamente que sus contrapartes de los Estados Unidos, se inclinan por lo general a admitir la utilización de cualquier método de firma o autenticación electrónicas, incluso sin que lo autorice una

---

fraude, no porque en los correos propiamente tales no sirvieran para consignar válidamente las condiciones de un contrato, sino porque no había indicios de que los autores de los correos electrónicos ni las personas mencionadas en ellos fueran empleados del demandado.

[51] *Roger Edwards, LLC* contra *Fiddes & Son, Ltd.,* Tribunal de distrito de los Estados Unidos, Distrito de Maine, 14 de febrero de 2003, *Federal Supplement*, segunda serie, vol. 245, pág. 251.

[52] *Hall* contra *Cognos Limited* (*Hull Industrial Tribunal*, causa Nº 1803325/97) (sin documentar).

[53] *Mehta* contra *J. Pereira Fernandes S.A*. [2006] EWHC 813 (Ch), (Reino Unido, Tribunal superior de Inglaterra y Gales, *Chancery Division*), [2006] 2 *Lloyd's Rep* 244 (Reino Unido, Inglaterra y Gales, *Lloyd's List Law Reports*).

[54] *Pretty Pictures Sarl* contra *Quixote Films Ltd.*, 30 de enero de 2003 ([2003] EWHC 311 (QB), (Reino Unido, Tribunal Superior de Inglaterra y Gales, *Law Reports Queen's Bench*, [2003] *All* ER (D) 303 (enero)) (Reino Unido, *All England Direct Law Reports* (*Digests*)).

[55] *Mehta* contra *J. Pereira Fernandes S.A*. (véase la nota [55]).

legislación determinada, siempre que el método en cuestión cumpla la misma función que la firma manuscrita[56].

32. Los tribunales de los ordenamientos de tradición jurídica romanista tienden a aplicar un enfoque más restrictivo, posiblemente porque en muchos de ellos el concepto de "documento" supone habitualmente algún tipo de autenticación, lo que dificulta disociarlo de la "firma". Por ejemplo, los tribunales de Francia eran reacios a aceptar la equivalencia entre los medios electrónicos de identificación y la firma manuscrita hasta que se aprobó legislación por la que se reconocía expresamente la validez de la firma electrónica[57]. Se observa una postura ligeramente más flexible en algunos fallos en que se acepta la presentación electrónica de recursos administrativos para cumplir un plazo legal, al menos si se confirman posteriormente por correo ordinario[58].

33. A diferencia del criterio restrictivo aplicado a la asignabilidad de los mensajes de datos en la formación de un contrato, los tribunales alemanes han aceptado al parecer con mayor flexibilidad la equivalencia entre la firma manuscrita y los métodos de identificación a efectos de las actuaciones judiciales. En Alemania, el debate ha girado en torno a la utilización cada vez más frecuente de imágenes escaneadas de la firma del letrado para autenticar facsímiles de escritos de recurso transmitidos por módem directamente desde una computadora a la máquina de fax del tribunal. En casos anteriores, los tribunales de apelación[59] y el Tribunal Federal (*Bundesgerichtshof*)[60] habían sostenido que la imagen escaneada de una firma manuscrita no cumplía los requisitos en vigor relativos a la firma y no constituía prueba de la identidad. Era concebible que la identificación se relacionara con una "firma electrónica avanzada", según se definía en el derecho alemán. Sin embargo,

---

[56] *Mehta* contra *J. Pereira Fernandes S.A.* (véase la nota [55]), Nº 25: "cabe señalar que en opinión de la Comisión legislativa acerca de [la Directiva de la Unión Europea sobre el comercio electrónico (2003/31/CE)] no se requieren cambios importantes con respecto a las leyes por las que se exija la firma, porque el cumplimiento de ese requisito se puede demostrar funcionalmente determinando si el comportamiento del posible signatario indica la intención de autenticar para una persona razonable. ... Así pues, como he señalado, si una parte o su agente que envíen un correo electrónico mecanografían su nombre en el texto de un mensaje de correo electrónico, conforme a lo exigido o permitido por la jurisprudencia, a mi juicio ello constituiría firma a efectos de lo dispuesto en [la legislación sobre el fraude]".

[57] El Tribunal de Casación de Francia declaró inadmisible un recurso firmado electrónicamente, entendiendo que existían dudas respecto de la identidad de la persona que había creado la firma, y que el recurso se había firmado electrónicamente antes de la entrada en vigor de la ley de 13 de marzo de 2000, por la cual se reconocía la eficacia jurídica de las firmas electrónicas (Tribunal de casación, Segunda Sala de lo Civil, 30 de abril de 2003, *Sté Chalets Boisson c/ M. X.*, publicado en www.juriscom.net/jpt/visu.php?ID=239, consultado el 12 de septiembre de 2003).

[58] Francia, Consejo de Estado, 28 de diciembre de 2001, N° 235784, *Élections municipales d'Entre-Deux-Monts*, publicado en www.rajf.org/article.php3?id_article=467, consultado el 12 de septiembre de 2003.

[59] Por ejemplo, *Oberlandesgericht* (Tribunal de Apelación), *Karlsruhe*, causa Nº 14 U 202/96, 14 de noviembre de 1997, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 09/1998, publicado en www.jurpc.de/rechtspr/19980009.htm, consultado el 12 de septiembre de 2003.

[60] Alemania, *Bundesgerichtshof* (Tribunal Federal de Justicia), causa Nº XI ZR 367/97, 29 de septiembre de 1998, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok Nº 05/1999, publicado en http://www.jurpc.de/rechtspr/19990005.htm, consultado el 12 de septiembre de 2003.

en general, correspondía al legislador y no a los tribunales fijar las condiciones de la equivalencia entre los escritos y las comunicaciones intangibles transmitidas mediante transferencia de datos[61]. Esa decisión se revocó ulteriormente por la opinión unánime de otros tribunales federales superiores, que aceptaron la presentación de determinados escritos procesales en forma de mensajes de datos transmitidos por vía electrónica que llevaban una firma escaneada[62].

34. Es interesante observar que incluso los tribunales de algunos foros romanistas que han promulgado leyes favorables a la utilización de firmas digitales basadas en una ICP, como Colombia[63], han adoptado un criterio igualmente flexible y confirmado, por ejemplo, la admisibilidad de actuaciones judiciales realizadas íntegramente por medio de comunicaciones electrónicas. Las presentaciones intercambiadas durante dichas actuaciones eran válidas, incluso si no llevaban firma digital, porque en las comunicaciones se utilizaban métodos que permitían identificar a las partes[64].

35. Todavía no hay mucha jurisprudencia sobre la firma electrónica, y los pocos fallos judiciales pronunciados hasta ahora no constituyen base suficiente para sacar conclusiones firmes. Como fuere, un breve examen de los precedentes pone de manifiesto varias tendencias. Al parecer, el criterio legislativo adoptado respecto de la firma y la autenticación electrónicas ha influido en la actitud de los tribunales al respecto. Cabe afirmar que el hincapié legislativo en las "firmas" electrónicas, sin una norma general relativa a la autoría, ha hecho que se preste demasiada atención a la función de los métodos de autenticación relativa a la identidad. En algunos países, ello ha generado cierta desconfianza respecto de los métodos de autenticación que no corresponden a la definición legislativa de "firma" electrónica.

---

[61] Ibíd.

[62] En un fallo relativo a una causa que le remitió el *Bundesgerichtshof* (Tribunal Federal de Justicia) de Alemania (véase la nota [62]), el *Gemeinsamer Senat der obersten Gerichtshöfe des Bundes* (Sala conjunta de los tribunales federales superiores de Alemania) observó que en las actuaciones judiciales el requisito de forma no era un fin en sí mismo. Su finalidad era garantizar una determinación suficientemente fiable ("*hinreichend zuverlässig*") del contenido del escrito y la identidad de la persona de que emanaba. La Sala conjunta tomó nota de la evolución práctica de los requisitos de forma para dar cabida a adelantos tecnológicos anteriores como el télex o el fax. La Sala conjunta sostuvo que aceptar ciertas presentaciones procesales por medio de la comunicación electrónica de un mensaje de datos en que constara la imagen escaneada de una firma concordaría con el espíritu de la jurisprudencia existente (*Gemeinsamer Senat der obersten Gerichtshöfe des Bundes*, *GmS-OGB 1/98*, 5 de abril de 2000, JurPC *Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 160/2000, publicado en http://www.jurpc.de/rechtspr/20000160.htm, consultado el 12 de septiembre de 2003).

[63] Por ejemplo, Colombia, que adoptó la Ley Modelo de la CNUDMI sobre Comercio Electrónico, incluidas las disposiciones generales del artículo 7, pero estableció la presunción legal de autenticidad únicamente con respecto a la firma digital (Colombia, Ley de comercio electrónico, art. 28).

[64] Colombia, Juzgado Segundo Promiscuo Municipal Rovira Tolima, *Juan Carlos Samper* contra *Jaime Tapias*, 21 de julio de 2003, Rad. 73-624-40-89-002-2003-053-00. El tribunal dictaminó que las actuaciones realizadas electrónicamente eran válidas incluso si los correos electrónicos no llevaban firma digital, porque a) podía identificarse plenamente al remitente de los mensajes de datos; b) este remitente reconocía y reafirmaba el contenido de los mensajes de datos enviados; c) los mensajes de datos se conservaban de forma segura en el tribunal; y d) los mensajes podían examinarse en cualquier momento (publicado en http://www.camara-e.net/_upload/80403--0-7-diaz082003.pdf, consultado el 2 de febrero de 2007).

Por ello, es dudoso que los mismos tribunales que han adoptado un criterio flexible respecto de los recursos de apelación judiciales o administrativos lo aplicaron igualmente en cuanto a los requisitos de firma para establecer la validez de un contrato. Ciertamente, aunque en el marco de un contrato una parte podía encarar el peligro de rechazo del acuerdo por la otra parte, en el contexto de las actuaciones civiles suelen ser la parte que utiliza una firma o un registro electrónico la que está interesada en confirmar la aprobación de este registro y su contenido.

3. Tentativas de crear equivalentes electrónicos de firmas especiales

a) Apostillas*

36. Se ha señalado que la letra y el espíritu del Convenio sobre la Eliminación del Requisito de la Legalización de Documentos Públicos Extranjeros, hecho en La Haya el 5 de octubre de 1961, no era obstáculo para utilizar tecnología moderna[65]. En el Primer Foro Internacional sobre certificación notarial y apostillas electrónicas se refrendó esta conclusión y se señaló que la aplicación y el funcionamiento del Convenio podían mejorarse utilizando dichas tecnologías[66]. Si se interpreta este instrumento según el principio de la equivalencia funcional, los organismos competentes podrían llevar registros electrónicos y expedir apostillas electrónicas, para reforzar la asistencia judicial internacional y los servicios estatales.

37. En abril de 2006, la Conferencia de La Haya de Derecho Internacional Privado y la Asociación Nacional de Notarios (NNA) de los Estados Unidos pusieron en marcha el programa experimental de apostillas electrónicas (*e-APP*). En el marco de dicha iniciativa, la Conferencia y la Asociación, conjuntamente con los Estados interesados, realizan actividades para elaborar, promover y apoyar modelos informáticos destinados a: a) expedir y utilizar apostillas electrónicas (apostillas-e) y b) utilizar registros electrónicos de apostillas (registros-e)[67].

---

* Se podría continuar ampliando esta sección en una versión final del documento general de consulta.

[65] Conferencia de La Haya de Derecho Internacional Privado, "Conclusiones y recomendaciones adoptadas por la Comisión Especial sobre el funcionamiento práctico de los convenios de La Haya sobre apostillas, obtención de pruebas y notificación, 28 de octubre a 4 de noviembre de 2003" (La Haya, 2003).

[66] Conclusiones aprobadas durante el Primer Foro Internacional sobre la Notarización y las Apostillas Electrónicas, celebrado en Las Vegas (Estados Unidos) los días 30 y 31 de mayo de 2005, y publicadas en el sitio http://www.hcch.net/upload/concl_forum.pdf, consultado el 7 de febrero de 2007.

[67] El e-*APP* está concebido para utilizarse con tecnología existente y común. La que se propone se basa en el sistema *Portable Document Format* (PDF), al que se incorpora el de *Extensible Markup Language* (XML). Para obtener más información al respecto, consúltese el sitio http://hcch.e-vision.nl/index_en.php?act=text.display&tid=37, en "*Second International Forum on e-Notarization and e-Apostilles*", celebrado en Washington, D.C., del 27 al 29 de mayo de 2006.

b) Sellos

38. En algunos foros ya se eliminó el requisito de los sellos, porque ya no están a la altura de los tiempos. Se reemplazaron por la firma atestada (esto es, atestiguada)[68]. En otros foros hay leyes por las que la firma electrónica segura cumple los requisitos de sellado. Por ejemplo, en Irlanda existen disposiciones expresas relativas a las firmas electrónicas seguras, con certificación apropiada, que pueden utilizarse en lugar de sellos, con el consentimiento de la persona o el organismo público a que se debe o se puede presentar el documento sellado[69]. En el Canadá se prevé que los requisitos del sello de una determinada persona con arreglo a algunas leyes federales se cumplan mediante una firma electrónica segura que constituye el sello de esa persona[70].

39. Además, en varios países se han puesto en marcha iniciativas en que se prevé la utilización de documentos y firmas electrónicas en transacciones de terrenos relacionadas con títulos. Conforme al modelo utilizado en Victoria (Australia), se utiliza tecnología de firma digital segura por Internet mediante tarjetas digitales expedidas por una autoridad de certificación. En el Reino Unido, conforme al modelo se prevé el otorgamiento de un título por los abogados en nombre de sus clientes por medio de una Intranet. En algunos ordenamientos jurídicos, la legislación reconoce la posibilidad de utilizar "sellos electrónicos" en lugar de "sellos manuales", y deja pendientes para su determinación por separado los aspectos técnicos de la forma del sello electrónico[71].

---

[68] Por ejemplo, en la Ley sobre la propiedad (disposiciones generales) del Reino Unido de 1989, por la que se aplicó el informe de la *Law Reform Commission* sobre "*Deeds and escrows*" (*Law Com.* Nº 143, 1987).

[69] Irlanda, Ley de comercio electrónico, artículo 16. Sin embargo, si el documento sellado debe o puede entregarse a un órgano público o a una persona que actúe en nombre de un órgano público, el órgano público que acepte la utilización de una firma electrónica podrá exigir que ésta se ajuste a determinados requisitos de tecnología de la información y de procedimiento.

[70] Canadá, Ley de protección de la información personal y los documentos electrónicos (2000), segunda parte, artículo 39. Las leyes federales a que se alude son la Ley Federal de Bienes Inmuebles y el Reglamento Real federal sobre bienes inmuebles.

[71] Ejemplos de ello son los requisitos relativos a la validación de documentos por profesionales autorizados o registrados, como la Ley sobre los profesionales de la ingeniería y las geociencias (Manitoba (Canadá)), en que se define el "sello electrónico" como la forma de identificación expedida por la asociación de cualquier miembro que se utilizará para validar electrónicamente los documentos en un formato legible por computadora (véase http://apegm.mb.ca/keydocs/act/index.html, consultado el 4 de abril de 2007).

40. La Ley Uniforme sobre el registro electrónico de bienes raíces de los Estados Unidos[72] señala expresamente que la imagen física o electrónica de un timbre, impresión o sello no tiene que acompañar necesariamente una firma electrónica. En lo esencial, lo que se requiere es únicamente la información que figura en el sello antes que este sello propiamente dicho. Además, se dispone que toda ley, reglamento o norma que exija la presencia de un timbre, impresión o sello personal o empresarial se cumplirá mediante una firma electrónica. Estos indicios físicos no se pueden aplicar a un documento totalmente electrónico. No obstante, esta ley requiere que la información que de otro modo figuraría en el timbre, la impresión o el sello se debe adjuntar o asociar lógicamente al documento o firma de manera electrónica[73]. De este modo, el timbre o impresión notarial exigidos con arreglo a la ley de algunos Estados no se requieren en el caso de una certificación notarial electrónica con arreglo a esta ley. Tampoco es necesario que se verifique la acción del funcionario de una empresa mediante un timbre o impresión correspondiente a ella, como se requeriría en otros casos conforme a la legislación de algunos Estados.

c) Certificación notarial*

41. En los Estados Unidos hay tres leyes principales sobre la certificación notarial: la Ley Uniforme de operaciones electrónicas, la Ley sobre firma electrónica en el comercio mundial y nacional (firma-e)[74] y la Ley Uniforme sobre el registro de operaciones inmobiliarias[75]. En su conjunto, disponen que se cumplen los requisitos legales para que se certifique notarialmente, reconozca, verifique, atestigüe o cree bajo juramento un documento, o una firma correspondiente a él, si la firma electrónica de la persona autorizada para realizar dichos actos, junto con toda otra información que se deba incorporar conforme al derecho aplicable, se adjuntan al documento o la firma o se asocian lógicamente con éste.

42. En Austria, el archivo de documentos electrónicos *cyberDOC*, empresa independiente establecida conjuntamente por la Cámara de Notarios de Derecho Civil de Austria y Siemens AG, suministra a los notarios un archivo electrónico que comprende funciones de autenticación[76]. Los notarios austríacos están obligados por ley a registrar y almacenar en este archivo todas las actas notariales validadas después del 1º de enero de 2000.

---

[72] La Ley uniforme sobre el registro electrónico de operaciones inmobiliarias de los Estados Unidos fue elaborada por la Conferencia Nacional de Comisarios de Leyes Uniformes de los Estados, y se publicó en el sitio http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm, consultado el 7 de febrero de 2007. Se aprobó en Arizona, Carolina del Norte, Delaware, el Distrito de Columbia, Kansas, Texas, Virginia y Wisconsin (véase http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-urpera.asp, consultado el 7 de febrero de 2007).

[73] Es decir, se trata de criterios análogos a los aplicados en la Ley Uniforme de operaciones electrónicas de los Estados Unidos.

* El contenido de esta sección podría ampliarse en la versión final del documento general de consulta.

[74] Codificada como título 15, capítulo 96, artículos 7001 a 7031 del Código de los Estados Unidos.

[75] Véase la nota [74].

[76] Véase *Österreichische Notariatskammer* (Cámara de Notarios de Derecho Civil de Austria), publicado en http://www.notar.at/de/portal/einrichtungen/cyberdocgmbhcokg/, consultado el 7 de febrero de 2007.

d) Atestación

43. Se ha afirmado que los procedimientos tradicionales de atestiguación, como la atestación, no son del todo adaptables al de la firma electrónica de documentos, porque no existen seguridades de que la imagen que aparece en la pantalla corresponde efectivamente al documento en que se estampará la firma electrónica. Lo único que ven el testigo y el firmante es una representación en pantalla, legible para una persona normal, de lo que se halla presuntamente almacenado en la memoria. Cuando el testigo observa al firmante en el momento en que pulsa el teclado, no sabe con certeza lo que está ocurriendo. Por ello, sólo sería posible asegurar que la imagen de la pantalla corresponde al contenido de la memoria del ordenador, y que las pulsaciones del firmante reflejan sus intenciones si este ordenador ha sido evaluado según criterios fiables para determinar que sigue una trayectoria fiable[77].

44. Sin embargo, la firma electrónica segura cumpliría una función análoga a la del testigo atestador al identificar a la persona que supuestamente firma el documento. Al utilizar una firma electrónica segura**, sin un testigo**, sería posible verificar la autenticidad de esa firma, la identidad de la persona a que pertenece, la integridad del documento y, probablemente, incluso la fecha y la hora de la firma. En este sentido, la firma electrónica segura puede ser mejor incluso que la firma manuscrita corriente. Las ventajas de contar, además, con un testigo real que diera fe de una firma digital segura serían tal vez ínfimas, a menos que se hallara en duda el carácter voluntario de la firma[78].

45. La legislación en vigor no ha llegado a sustituir enteramente los requisitos de atestación por la firma electrónica, sino que permite meramente que el testigo la utilice. La Ley de operaciones electrónicas de Nueva Zelandia establece que la firma electrónica de un testigo basta para dar validez legal a una firma o un sello. No se indica la tecnología que se debe utilizar para estampar la firma electrónica, siempre que con ésta "se identifique correctamente al testigo y se señale que se ha dado fe de la firma o el sello", así como que "su grado de fiabilidad corresponde a los fines y las circunstancias para los que se requiere la firma del testigo"[79].

---

[77] En las publicaciones especializadas, esta situación se denomina, en inglés, "*What you see is what you sign*" (WYSIWYS) ("Lo que ves es lo que firmas"). Véase V. Liu y otros, "*Visually sealed and digitally signed documents*", *Association of Computing Machinery*, *ACM International Conference Proceedings Series*, vol. 56, *Proceedings of the Twenty-seventh Australasian Conference on Computer Science*, vol. 26, (Dunedin, Nueva Zelandia, 2004) pág. 287 (en el mismo documento se examinan también los controladores de visualización fiables).

[78] Véanse los análisis *Joint IDA-AGC Review of Electronic Transactions Act Stage II: Exclusions under Section 4 of the ETA*, del Organismo de Desarrollo del Sector de la información y la Comunicación de Singapur y el Gabinete del Fiscal General, documento de consulta LRRD Nº 2/2004 (Singapur, 2004), quinta y octava parte, publicado en la sección "Publications" del sitio www.agc.gov.sg.

[79] Nueva Zelandia, Ley de operaciones electrónicas (véase la nota [9]), artículo 23, publicado en http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes, consultado el 4 de abril de 2007.

46. La Ley de protección de la información personal y documentos electrónicos del Canadá dispone que los requisitos de la legislación federal para la atestación de una firma se cumplen con respecto a un documento electrónico si todos los firmantes y testigos estampan su firma electrónica segura en dicho documento electrónico[80]. Podrá hacerse en formato electrónico una declaración que exigen algunas leyes federales en que se indique o certifique que toda información suministrada por la persona que hace dicha declaración es verdadera, exacta o completa si esta persona estampa en ella su firma electrónica segura[81]. La declaración que debe hacerse bajo juramento o por afirmación solemne con arreglo a la legislación federal podrá efectuarse en forma electrónica si su autor estampa en ella su firma electrónica segura, y si la persona ante quien se efectúe dicha declaración, y se halle autorizada para recibirla en virtud de un juramento o afirmación solemne, estampa a su vez en ella su firma electrónica segura[82]. Una de las opciones que se han propuesto para dar más seguridades es que la firma electrónica sea estampada por un profesional fiable, como un abogado o notario o en su presencia[83].

---

[80] Canadá, Ley de protección de la información personal y documentos electrónicos (véase la nota [72]), segunda parte, artículo 46.

[81] Ibíd., artículo 45.

[82] Ibíd., artículo 44.

[83] Los especialistas en transmisión de bienes inmuebles deberán obtener una firma electrónica y recibir autenticación de un organismo de certificación reconocido. Tal vez los compradores y vendedores tengan que extenderles poderes por escrito para que estampen su firma. Véase "*E-conveyancing: the strategy for the implementation of e-conveyancing in England and Wales*" (Reino Unido, Registro de la Propiedad, 2005), publicado en http://www.landregistry.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc, consultado el 7 de abril de 2007. Se prevé ejecutar el proyecto por etapas entre 2006 y 2009.