CNUDMI
COMISIÓN DE LAS NACIONES UNIDAS
PARA EL DERECHO MERCANTIL INTERNACIONAL

Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas

NACIONES UNIDAS

COMISIÓN DE LAS NACIONES UNIDAS
PARA EL DERECHO MERCANTIL INTERNACIONAL

Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas

NACIONES UNIDAS
Viena, 2009

PUBLICACIÓN DE
LAS NACIONES UNIDAS
Núm. de venta: S.09.V.4
ISBN 978-92-1-133663-4

Prefacio

Cuando finalizó su labor relacionada con la Convención sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, en 2004, el Grupo de Trabajo IV (Comercio Electrónico) de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) pidió a la Secretaría que siguiera de cerca diversas cuestiones relacionadas con el comercio electrónico, incluidas las relativas al reconocimiento transfronterizo de las firmas electrónicas, y publicara los resultados de sus investigaciones con miras a formular recomendaciones a la Comisión respecto de una posible labor futura en esas esferas (A/CN.9/571, párr. 12).

En 2005, la CNUDMI tomó nota de la labor realizada por otras organizaciones en diversos ámbitos relacionados con el comercio electrónico y pidió a la Secretaría que preparara un estudio más detallado en el que se incluyeran propuestas sobre la forma y la naturaleza de un documento general de referencia en el que se examinaran los diversos elementos necesarios para establecer un marco jurídico favorable al comercio electrónico, que la Comisión tal vez pudiera plantearse preparar en el futuro con miras a prestar asistencia a los legisladores y los encargados de formular las políticas en todo el mundo[1].

En 2006, la CNUDMI examinó una nota preparada por su secretaría atendiendo a esa solicitud (A/CN.9/604). En la nota se señalaban las siguientes esferas como posibles elementos de un documento general de referencia: *a)* autenticación y reconocimiento transfronterizo de las firmas electrónicas; *b)* responsabilidad y normas de conducta para los prestadores de servicios de información; *c)* facturación electrónica y cuestiones jurídicas relacionadas con las cadenas de suministro en el comercio electrónico; *d)* transferencia de derechos sobre bienes corporales y otros derechos mediante comunicaciones electrónicas; *e)* competencia desleal y prácticas comerciales engañosas en el comercio electrónico; y *f)* protección de la esfera privada y de los datos en el comercio electrónico. En la nota también se indicaban otras cuestiones que podrían incluirse en un documento de esta índole, si bien de forma más resumida, a saber: *a)* protección de los derechos de propiedad intelectual; *b)* comunicaciones electrónicas no solicitadas ("spam"); y *c)* ciberdelincuencia. En aquel período de sesiones se apoyó la opinión de que tal vez se facilitaría considerablemente la tarea de los legisladores y formuladores de políticas, en particular en los países en desarrollo, si la CNUDMI preparaba un documento general de referencia que se ocupara de los temas señalados por la Secretaría. También se afirmó que ese documento podría servir de ayuda a la CNUDMI para concretar esferas en la que la propia Comisión pudiera emprender una labor de armonización en el futuro. La CNUDMI pidió a la Secretaría

[1] *Documentos Oficiales de la Asamblea General, sexagésimo período de sesiones, Suplemento Nº 17* (A/60/17), párr. 214.

que preparase un modelo de parte del documento general de referencia que se ocupara específicamente de cuestiones relacionadas con la autenticación y el reconocimiento transfronterizo de las firmas electrónicas para examinarlo en su 40º período de sesiones, en 2007[2].

El modelo de capítulo que preparó la Secretaría atendiendo la petición mencionada (A/CN.9/630 y Add. 1 a 5) se presentó a la CNUDMI para su examen en su cuadragésimo período de sesiones. La Comisión elogió a la Secretaría por el modelo de capítulo preparado y le pidió que lo diera a conocer como publicación independiente[3].

En la presente publicación se analizan las principales cuestiones jurídicas que se plantean en la utilización de métodos de firma y autenticación electrónicas en las transacciones internacionales. En la primera parte se examinan en general los métodos empleados para la firma y la autenticación electrónicas y su consideración jurídica en diversos foros. En la segunda parte se examina la utilización de los métodos de firma y autenticación electrónicas en las transacciones internacionales y se determinan las principales cuestiones jurídicas relacionadas con el reconocimiento transfronterizo de esos métodos. Se ha observado que, desde una perspectiva internacional, es más probable que surjan dificultades jurídicas en relación con la utilización transfronteriza de los métodos de firma y autenticación electrónicas que requieran la participación de terceros en el proceso de firma o autenticación. Así ocurre, por ejemplo, en el caso de los métodos de firma y autenticación electrónicas basados en certificados emitidos por un tercero de confianza prestador de servicios de certificación, en especial las firmas digitales de una infraestructura de clave pública (ICP). Por ello, la segunda parte de la presente publicación dedica atención especial a la utilización internacional de las firmas digitales en el marco de una infraestructura de clave pública. Esta atención no debe entenderse como preferencia o apoyo de este o cualquier otro tipo de método o tecnología de autenticación.

[2]Ibíd., *sexagésimo primer período de sesiones Suplemento Nº 17* (A/61/17), párr. 216.

[3]Ibíd., *sexagésimo segundo período de sesiones, Suplemento Nº 17* (A/62/17), párr. 195.

Índice

Introducción

1. En las tecnologías de la información y la informática se han puesto a punto diversos medios de vincular la información en forma electrónica a personas o entidades concretas, con objeto de garantizar la integridad de dicha información o de permitir que las personas demuestren su derecho o autorización para obtener acceso a un determinado servicio o depósito de información. Estas funciones suelen denominarse genéricamente métodos de "autenticación" electrónica o de "firma" electrónica. Ahora bien, en ocasiones se establecen distinciones entre la "autenticación" electrónica y la "firma" electrónica. El empleo de la terminología no sólo es poco sistemático, sino en cierta medida engañoso. En un entorno basado en el papel, las palabras "autenticación" y "firma" y los actos conexos de "autenticar" y "firmar" no tienen exactamente el mismo matiz en distintos ordenamientos jurídicos y poseen funciones que no tienen por qué corresponderse con el propósito y la función de los métodos electrónicos de "autenticación" y "firma". Además, en ocasiones se utiliza la palabra "autenticación" de forma genérica en relación con el aseguramiento de la autoría y la integridad de la información, pero cabe la posibilidad de que algunos ordenamientos jurídicos establezcan distinciones entre esos elementos. Así pues, es necesario presentar una breve reseña de las diferencias de terminología y de interpretación jurídica a fin de determinar el alcance del presente documento.

2. Conforme al derecho anglosajón sobre las pruebas en lo civil, se considera que una información consignada o un documento es "auténtico" si existen pruebas de que el documento o la información consignada "es lo que afirma el proponente"[1]. La noción de "documento" como tal es bastante amplia y suele abarcar "cualquier cosa en la que se consigne información de cualquier tipo"[2], lo que incluiría por ejemplo, elementos como fotografías de lápidas y casas[3], libros de contabilidad[4], y dibujos y planos[5]. La pertinencia de un documento como elemento de prueba se establece al vincularlo a una persona, lugar o cosa, proceso que en algunos foros de derecho anglosajón se denomina "autenticación"[6]. Firmar un documento es un medio habitual —aunque no

[1] Estados Unidos de América, Reglamento Federal sobre las pruebas, regla 901 *a)*: "El requisito de autenticación o identificación como condición suspensiva de la admisibilidad se cumple mediante pruebas suficientes que apoyen una constatación de que el asunto en cuestión es lo que afirma su proponente".

[2] Reino Unido de Gran Bretaña e Irlanda del Norte, Ley de pruebas en lo civil de 1995, capítulo 38, artículo 13.

[3] *Lyell contra Kennedy (Nº 3)* (1884) 27 Ch.D.1 (Reino Unido, Chancery Division).

[4] *Hayes contra Brown* [1920] 1 K.B. 250 (Reino Unido, Law Reports, King's Bench).

[5] *J. H. Tucker & Co., Ltd. contra. Board of Trade* [1955] 2 All ER 522. (Reino Unido, All England Law Reports).

[6] *Farm Credit Bank of St. Paul contra William G. Huether*, 12 de abril de 1990 (454 N.W.2d 710, 713) (Estados Unidos, Corte Suprema de Dakota del Norte, North Western Reporter).

exclusivo— de "autenticación", y, según el contexto, las expresiones "firmar" y "autenticar" pueden utilizarse como sinónimos[7].

3. A su vez, una "firma" es "todo nombre o símbolo utilizado por una parte con la intención de que constituya su firma"[8]. Cabe entender que la finalidad de las normas legales que prescriben que un documento concreto sea firmado por una persona concreta es confirmar la autenticidad del documento[9]. El paradigma de la firma es el nombre del firmante, escrito de su propio puño y letra, en un documento de papel (una firma "autógrafa" o "manuscrita")[10]. No obstante, la firma autógrafa no es el único tipo de firma concebible. Como los tribunales consideran las firmas "únicamente una marca", salvo que la norma legal en cuestión exija que la firma sea autógrafa, "es suficiente el nombre impreso de la parte que esté obligada a firmar el documento", o la firma "se podrá estampar en el documento mediante un sello grabado con un facsímil de la firma normal de la persona que firma", siempre que en estos casos se aporten pruebas "de que el nombre impreso en el sello fue puesto por la persona que firma", o que dicha firma "ha sido reconocida y se le ha hecho saber que se ha realizado con su autoridad para consignarla en el instrumento concreto"[11].

4. Los requisitos legales de firma como condición para la validez de determinados actos en foros de derecho anglosajón figuran por ejemplo en la Ley contra el Fraude británica[12] y sus versiones en otros países[13]. Con el transcurso del tiempo, frecuentemente los tribunales han dado una interpretación liberal a la Ley contra el Fraude, al reconocer que sus estrictos requisitos de forma se concibieron en un contexto concreto[14] y que la estricta observancia de sus disposiciones podría privar innecesariamente

---

[7] En el contexto del artículo 9 revisado del Código de Comercio Uniforme de Estados Unidos, por ejemplo, "autenticar" se define como "A) firmar, o B) ejecutar o adoptar de otra forma un símbolo, o cifrar o procesar de forma análoga una información consignada en todo o en parte, con la intención presente de la persona que autentica de identificarse y adoptar o aceptar una información consignada".

[8] *Alfred E. Weber contra Dante De Cecco*, 14 de octubre de 1948 (1 N.J. Super. 353, 358) (Estados Unidos, New Jersey Superior Court Reports).

[9] *Lobb contra Stanley* (1844), 5 Q.B. 574, 114 E.R. 1366 (Reino Unido, Law Reports, Queen's Bench).

[10] Lord Denning en *Goodman contra Eban* [1954] Q.B.D. 550 at 56: "En el uso inglés moderno, cuando se requiere que un documento esté firmado por una persona, ello significa que la persona debe escribir su nombre en el documento de su puño y letra." (Reino Unido, Queen's Bench Division).

[11] *R. contra Moore: ex parte Myers* (1884) 10 V.L.R. 322 at 324 (Reino Unido, Victorian Law Reports).

[12] La Ley contra el Fraude se promulgó en Gran Bretaña en 1677 "para la prevención de muchas prácticas fraudulentas que se trata habitualmente de llevar a cabo mediante perjurio e incitación a cometer perjurio". La mayoría de sus disposiciones fueron derogadas en el Reino Unido durante el siglo XX.

[13] Por ejemplo, el artículo 2-201, párrafo 1, del Código de Comercio Uniforme de los Estados Unidos, que ha expresado la Ley contra el Fraude del siguiente modo: "Salvo que el presente artículo disponga otra cosa, un contrato de compraventa de bienes por un precio de 500 dólares o más no es ejecutorio por vía de acción o de excepción si no existe suficiente prueba por escrito que indique que se ha perfeccionado un contrato de venta entre las partes y ha sido firmado por una parte contra la que se solicita la ejecución o por su agente o intermediario autorizado".

[14] "La Ley contra el Fraude fue promulgada en un período en que el poder legislativo se inclinaba a disponer que las causas se decidieran con arreglo a reglas fijas, en lugar de permitir que el jurado considerara el efecto de las pruebas en cada caso. Sin duda, esta circunstancia emanó en cierta medida del hecho de que en aquella época el demandante y el demandado no eran testigos competentes". (J. Roxborough en *Leeman contra Stocks* [1951] 1 Ch 941 at 947-8) (Reino Unido, Law Reports, Chancery Division) citando con aprobación las opiniones de J. Cave en *Evans contra Hoare* [1892] 1 QB 593 at 597) (Reino Unido, Law Reports, Queen's Bench).

a los contratos de su efecto jurídico[15]. Así pues, en los últimos 150 años, se ha producido en los foros de derecho anglosajón una evolución del concepto de "firma", del hincapié original en la forma a la importancia de la función[16]. Los tribunales ingleses han considerado periódicamente variaciones de este tema, que van desde sencillas modificaciones como cruces[17] o iniciales[18], pasando por seudónimos[19] y frases identificadoras[20], hasta nombres impresos[21], firmas de terceros[22] y sellos de caucho[23]. En todos estos casos, los tribunales han podido resolver la cuestión de si se había efectuado una firma válida al compararla con una firma manuscrita. Así pues, podría afirmarse que en un contexto de algunos requisitos generales de forma rígidos, los tribunales en los foros de derecho anglosajón se han inclinado por formular una interpretación amplia de lo que significan las nociones de "autenticación" y "firma", centrándose en la intención de las partes y no en la forma de sus actos.

5. El enfoque de la "autenticación" y la "firma" en los foros romanistas no es idéntico en todos los respectos al enfoque del derecho anglosajón. La mayoría de los foros romanistas adoptan la regla de la libertad de forma para compromisos contractuales en asuntos de derecho privado, ya sea de forma expresa[24] o implícita[25], a reserva, no

---

[15] Como explicó Lord Bingham de Cornhill: "Enseguida fue patente que si la solución del siglo XVII hacía frente a un perjuicio, también era capaz de dar lugar a otro, a saber: que una parte, actuando sobre la base de lo que se suponía que era un acuerdo oral vinculante, vería frustradas sus expectativas comerciales cuando llegara el momento de la ejecución y la otra parte se sirviera de la falta de un memorando o nota del acuerdo por escrito". (*Actionstrength Limited contra International Glass Engineering*, 3 de abril de 2003, [2003] UKHL 17) (Reino Unido, Cámara de los Lores).

[16] Chris Reed, "What is a Signature?", *The Journal of Information, Law and Technology*, Vol. 3 (2000), con remisiones a jurisprudencia, disponible en http://www2.warwick.ac.uk/ fac/soc/law/elj/jilt/2000_3/ reed/, (consultado el 5 de junio de 2008).

[17] *Baker contra Dening* (1838) 8 A. & E. 94. (Reino Unido, Adolphus and Ellis' Queen's Bench Reports).

[18] *Hill contra Hill* [1947] Ch 231 (Reino Unido, Chancery Division).

[19] *Redding, in re* (1850) 14 Jur. 1052, 2 Rob. Ecc. 339 (Reino Unido, Jurist Reports y Robertson's Ecclesiastical Reports).

[20] Cook, In the Estate of (Deceased) Murison contra Cook and Another [1960] 1 All ER 689 (Reino Unido, All England Law Reports).

[21] *Brydges contra Dicks* (1891) 7 T.L.R. 215 (citado en *Brennan contra Kinjella Pty Ltd*. Tribunal Supremo de Nueva Gales del Sur, 24 de junio de 1993, 1993 NSW LEXIS 7543, 10). También se ha considerado la mecanografía en *Newborne contra Sensolid (Great Britain), Ltd*. [1954] 1 QB 45 (Reino Unido, Law Reports, Queen's Bench).

[22] *France contra Dutton*, 24 de abril de 1891 [1891] 2 QB 208 (Reino Unido, Law Reports, Queen's Bench).

[23] Goodman contra J. Eban Ltd., [1954] 1 QB 550, citado en Lazarus Estates, Ltd. contra Beasley, Tribunal de Apelación, 24 de enero de 1956 ([1956] 1 QB 702); London County Council contra Vitamins, Ltd., London County Council contra Agricultural Food Products, Ltd., Tribunal de Apelación, 31 de marzo de 1955 [1955] 2 QB 218 (Reino Unido, Law Reports, Queen's Bench).

[24] Así lo reconoce, por ejemplo, el artículo 11, párrafo 1 del Code des Obligations suizo. Igualmente, el artículo 215 del Código Civil alemán dispone que los acuerdos son inválidos únicamente si no se observó en ellos una forma prescripta por la ley o convenida por las partes. Con excepción de esos casos concretos, generalmente se interpreta que los contratos de derecho privado no están sujetos a requisitos de forma específicos. Cuando la ley prescribe expresamente una forma concreta, ese requisito ha de interpretarse estrictamente.

[25] En Francia, por ejemplo, la libertad de forma es un corolario de las reglas básicas sobre formación de contratos en virtud del Código Civil. De conformidad con el artículo 1108 del Código Civil francés, para que un contrato sea válido se exige el consentimiento del promitente, su capacidad jurídica, un determinado objeto y una causa lícita y, cuando se han cumplido esas condiciones, el contrato es "ley entre las partes" según el artículo 1134. Así ocurre también en España de conformidad con los artículos 1258 y 1278 del Código Civil. Italia adopta la misma norma, aunque de manera menos explícita (véase Codice Civile, artículos 1326 y 1350).

obstante de un catálogo más o menos amplio de excepciones que dependen del foro de que se trate. Esto significa que, por regla general, los contratos no tienen que ser "por escrito" o "firmados" para que sean válidos y ejecutorios. No obstante, existen foros romanistas que suelen exigir un escrito para demostrar el contenido de los contratos, salvo en cuestiones comerciales[26]. A diferencia de los foros de derecho anglosajón, los países de tradición romanista suelen interpretar las normas probatorias de una forma más bien estricta. Por lo general, las reglas sobre las pruebas en lo civil establecen una jerarquía probatoria para demostrar el contenido de los contratos civiles y comerciales. En los primeros lugares de esa clasificación figuran los documentos expedidos por autoridades públicas, seguidos de los documentos privados auténticos. A menudo, dicha jerarquía está concebida de manera que las nociones de "documento" y "firma", aunque distintas en la forma, pueden llegar a ser prácticamente inseparables[27]. No obstante, otros foros romanistas establecen un vínculo positivo entre la noción de "documento" y la existencia de una "firma"[28]. Esto no significa que un documento que no haya sido firmado quede privado forzosamente de valor probatorio, pero ese documento no sería objeto de ninguna presunción y se considera por lo general como "inicio de prueba"[29]. En la mayoría de los foros romanistas, la "autenticación" es un concepto que se interpreta de forma bastante estricta en el sentido de que la autenticidad de un documento ha sido verificada y certificada por una autoridad pública competente o un notario público. En el procedimiento civil es habitual referirse a la noción de la "originalidad" de los documentos.

6. Como ocurre en el caso del derecho anglosajón, en los países de tradición jurídica romanista el paradigma de una firma es la manuscrita. Por lo que se refiere a la firma propiamente dicha, algunos foros suelen admitir diversos equivalentes, entre ellos las reproducciones mecánicas de firmas, pese a que adoptan un enfoque generalmente formalista del proceso probatorio[30]. No obstante, otros foros aceptan las firmas mecánicas para operaciones comerciales[31], pero hasta la aparición de las tecnologías

[26] El artículo 1341 del Código Civil francés exige un escrito para la prueba de contratos por valor superior a una cierta cantidad, pero el artículo 109 del Código de Comercio admite diversos tipos de pruebas, sin jerarquía concreta. Por ello, la Cour de Cassation francesa reconoció en 1892 el principio general de la libertad de la prueba en asuntos comerciales (Cass. civ. 17 mai 1892, DP 1892.1.604; citado en Luc Grynbaum, *Preuve, Répertoire Commercial Dalloz*, junio de 2002, secciones 6 y 11)).

[27] Así pues, por ejemplo, de conformidad con el derecho alemán una firma no es elemento esencial de la noción de "documentos (Urkunde) (Gerhard Lüke und Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), artículo 415, Nº 6). No obstante, la jerarquía de pruebas documentales establecidas por los artículos 415, 416 y 419 del Código Procesal Civil alemán vincula claramente la firma al documento. Efectivamente, el artículo 416, sobre el valor probatorio de documentos privados (*Privaturkunden*) dispone que los documentos privados constituyen "prueba plena" de la información que contienen a condición de que estén firmados por el autor o por una firma protocolizada por notario. Como no existe una disposición relativa a los documentos sin firma, parece que comparten la suerte de los documentos con defectos de forma (es decir, indescifrables, dañados), cuyo valor probatorio es "establecido libremente" por los tribunales (Código Procesal Civil de Alemania, artículo 419).

[28] Así pues, en Francia la firma es un "elemento esencial" de los documentos privados ("*actes sous seing privé*") (véase *Recueil Dalloz, Preuve*, Nº 638).

[29] Este es el caso en Francia, por ejemplo (véase *Recueil Dalloz, Preuve*, Nºs 657 y 658).

[30] Los comentaristas del Código Procesal Civil de Alemania señalan que el requisito de una firma manuscrita significaría la exclusión de todas las formas de signos registrados mecánicamente, resultado que sería contrario a la práctica corriente y al progreso tecnológico (véase Gerhard Lüke y Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung*, (Munich, Beck, 1992, artículo 416, Nº 5).

[31] Por ejemplo, Francia (véase *Recueil Dalloz, Preuve*, Nº 662).

informáticas, siguieron exigiendo la firma manuscrita para la prueba de otros tipos de contratos[32]. Cabría por tanto afirmar que en un contexto general de libertad de forma para el perfeccionamiento de contratos mercantiles, los países de tradición jurídica romanista suelen aplicar normas estrictas para evaluar el valor probatorio de los documentos privados, y tal vez desestimen documentos cuya autenticidad no pueda reconocerse inmediatamente sobre la base de una firma.

7. El análisis precedente sirve para demostrar no sólo que las nociones de firma y autenticación no son objeto de una interpretación uniforme, sino que las funciones que cumplen son distintas de un sistema jurídico a otro. Pese a estas divergencias, pueden encontrarse unos pocos elementos generales comunes. En derecho, se suele interpretar que las nociones de "autenticación" y "autenticidad" se refieren a la autenticidad de un documento o una información consignada, es decir, que el documento es el soporte "original" de la información que contiene, en la forma en que se consignó y sin ninguna alteración. Las firmas, a su vez, cumplen tres funciones principales en el entorno basado en papel: las firmas permiten identificar al signatario (función de identificación); las firmas aportan certidumbre acerca de la participación personal de esa persona en el acto de la firma (función probatoria); y las firmas vinculan al signatario con el contenido de un documento (función de atribución). Cabe afirmar que las firmas pueden cumplir asimismo diversas otras funciones, según cual fuera la naturaleza del documento firmado. Por ejemplo, una firma puede constituir un testimonio de la intención de una parte de considerarse vinculada por el contenido de un contrato firmado; de la intención de una persona de respaldar la autoría de un texto (manifestando así su conciencia de que del acto de la firma podrían derivarse consecuencias jurídicas); de la intención de una persona de asociarse al contenido de un documento escrito por otra persona; y del hecho de que una persona estuviera en un lugar determinado en un momento determinado[33, 34].

8. Cabe señalar, no obstante, que aunque a menudo se presuma la autenticidad por existir una firma, la firma por sí sola no "autentica" un documento. Cabe que incluso los dos elementos se puedan separar, según las circunstancias. Una firma puede mantener su "autenticidad" incluso si el documento en el que está puesta se ha alterado posteriormente. Igualmente, un documento podrá ser "auténtico" aunque la firma que contiene sea falsa. Además, si bien es cierto que la autoridad para intervenir en una operación y la identidad real de la persona de que se trate son elementos importantes para garantizar la autenticidad de un documento o firma, no quedan demostrados plenamente por la firma por sí sola, ni constituyen suficiente garantía de la autenticidad de los documentos o de la firma.

---

[32] En Francia, por ejemplo, la firma no podía sustituirse por una cruz u otros signos, por un sello o por huellas dactilares (véase *Recueil Dalloz, Preuve*, Nº 665).

[33] *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001* (publicación de las Naciones Unidas, núm. de venta: S.02.V.8), segunda parte, párr. 29, disponible en http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html, (consultado el 6 de junio de 2008).

[34] Este análisis ya sirvió de base para los criterios de equivalencia funcional que figuran en el artículo 7 de la anterior Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guia para la Incorporación al Derecho Interno 1996, con el nuevo artículo 5 bis aprobado en 1998 (publicación de las Naciones Unidas, núm. de venta: S.99.V.4), disponible en http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html (consultado el 6 de junio de 2008).

9. Esta observación conduce a otro aspecto de la cuestión que se está examinando actualmente. Independientemente de la tradición jurídica de que se trate, una firma, con contadísimas excepciones, no es válida por sí misma. Su efecto jurídico dependerá del vínculo existente entre la firma y la persona a la que se atribuye la firma. En la práctica, pueden adoptarse varias medidas para verificar la identidad del firmante. Cuando todas las partes están presentes en el mismo lugar al mismo tiempo, se pueden reconocer mutuamente mirándose a la cara; si negocian por teléfono, podrán reconocer la voz del interlocutor, etc. Esto ocurre naturalmente y no está sometido a normas jurídicas concretas. Sin embargo, cuando las partes negocian por correspondencia, o cuando se transmiten documentos firmados por una cadena de contratación, tal vez existan pocos medios de determinar que los signos que figuran en un documento concreto fueron efectivamente realizados por la persona con cuyo nombre parecen estar vinculados y que, efectivamente, la persona debidamente autorizada fue la que produjo la firma que se supone obliga a una persona concreta.

10. Aunque una firma manuscrita es una forma habitual de "autenticación" y sirve para documentos de transacción que cambian de manos entre partes conocidas, en muchas situaciones comerciales y administrativas una firma es sin embargo relativamente insegura. La persona que confía en el documento no suele disponer de los nombres de las personas autorizadas a firmar ni de especimenes de sus firmas a efectos de comparación[35]. Esta situación es especialmente cierta en el caso de muchos documentos en los que se confía en países extranjeros en operaciones comerciales internacionales. Incluso cuando existe un espécimen de la firma autorizada con fines de comparación, tan solo un perito podrá detectar una falsificación bien hecha. Cuando se tramita un gran número de documentos, a veces ni siquiera se comparan las firmas, salvo cuando se trata de operaciones muy importantes. La confianza es uno de los elementos básicos de las relaciones comerciales internacionales.

11. La mayoría de los ordenamientos jurídicos cuentan con procedimientos o requisitos especiales concebidos para refrendar la fiabilidad de las firmas manuscritas. Algunos procedimientos pueden ser de obligado cumplimiento para que determinados documentos surtan efecto jurídicos. También pueden ser optativos y ser utilizados por las partes que deseen tomar medidas para excluir posibles argumentos sobre la autenticidad de determinados documentos. Entre los ejemplos característicos cabe citar los siguientes:

a) Certificación notarial. En determinadas circunstancias, el acto de la firma reviste una importancia formal concreta por la confianza reforzada que se asocia a una ceremonia especial. Así ocurre, por ejemplo, en el caso de la certificación notarial, es

[35] Algunos ámbitos del derecho reconocen tanto la inseguridad intrínseca de las firmas manuscritas como la inviabilidad de insistir en requisitos estrictos de forma para la validez de actos jurídicos, y admiten que en algunos casos incluso la falsificación de una firma no privaría a un documento de su efecto jurídico. Así pues, por ejemplo, el artículo 7 de la Ley Uniforme referente a las letras de cambio y pagarés a la orden anexa al Convenio por el que se establece una Ley uniforme referente a las letras de cambio y pagarés a la orden, hecho en Ginebra el 7 de junio de 1930, dispone que "si una letra de cambio lleva la firma de personas incapaces de obligarse en una letra de cambio, o firmas falsas, o firmas de personas imaginarias, o firmas que por cualquier otra razón no pueden obligar a las personas que han firmado la letra de cambio o en cuyo nombre aparezca firmada, las obligaciones de los demás firmantes no son por ello menos válidas" (Sociedad de las Naciones, *Treaty Series*, vol. CXLIII, Nº 3313).

decir, la certificación por un notario público para determinar la autenticidad de una firma en un documento legal, lo que a menudo requiere la comparecencia física de la persona ante el notario;

b) Atestación. Se entiende por atestación el acto de observar a una persona firmar un documento legal y seguidamente poner la propia firma como testigo. La finalidad de la atestación es conservar una prueba de la firma. Al atestar, el testigo declara y confirma que la persona a la que ha observado firmar el documento efectivamente lo hizo. La atestación no incluye la garantía de la exactitud o veracidad del documento. El testigo puede ser llamado a declarar sobre las circunstancias relativas a la firma[36];

c) Sellos. La práctica de utilizar sellos además de firmas, o en sustitución de éstas, no es insólita, especialmente en determinadas regiones del mundo[37]. La firma o la imposición de sellos pueden, por ejemplo, aportar pruebas de la identidad del firmante; que el firmante convino en obligarse por el acuerdo y lo hizo voluntariamente; que el documento es definitivo y cabal; o que la información no ha sido alterada después de la firma[38]. También podrá advertir al firmante e indicar la intención de actuar de forma jurídicamente vinculante.

12. Aparte de estas situaciones especiales, las firmas manuscritas se han utilizado en operaciones comerciales, tanto nacionales como internacionales, desde hace siglos sin ningún marco legislativo o funcional especialmente concebido. Los destinatarios o titulares de los documentos firmados han evaluado la fiabilidad de las firmas caso por caso según el nivel de confianza del firmante. De hecho, la inmensa mayoría de los contratos internacionales escritos —si es que hay "escritos"— no van acompañados forzosamente de un procedimiento especial en materia de forma o autenticación.

13. La utilización transfronteriza de documentos firmados se complica más cuando intervienen autoridades públicas, pues las autoridades receptoras de un país extranjero suelen exigir alguna prueba de la identidad y la autoridad del firmante. Por tradición, esos requisitos se cumplen por los denominados procedimientos de "legalización", en los que las firmas que figuran en documentos nacionales son autenticadas por las autoridades diplomáticas para su utilización en el extranjero. A la inversa, los representantes consulares o diplomáticos del país en el que se pretende utilizar los documentos también pueden autenticar las firmas de autoridades públicas extranjeras en el país de origen. A menudo, las autoridades consulares y diplomáticas autentican únicamente las firmas de determinadas autoridades de alto rango de los países de expedición, lo que exige varios niveles de reconocimiento de firmas cuando el documento fue expedido originalmente por un funcionario de menor rango, u obliga a la certificación notarial previa de las firmas por un notario del país emisor. En la mayoría de los casos, la legalización es un procedimiento engorroso, lento y costoso. Por ese motivo se

[36] Adrian McCullagh, Peter Little y William Caelli, "Electronic signatures: understand the past to develop the future", *University of New South Wales Law Journal*, vol. 21, Nº 2 (1998), véase el capítulo III, sección D, sobre el concepto de testificación.

[37] Se utilizan sellos en varios países de Asia oriental, como China y el Japón.

[38] Mark Sneddon, "Legislating to facilitate electronic signatures and records: exceptions, standards and the impact of the statute book", *University of New South Wales Law Journal*, vol. 21, Nº 2 (1998), véase la parte 2, capítulo II, sobre los objetivos normativos de los requisitos de escritura y firma.

negoció el Convenio sobre la Eliminación del Requisito de la Legalización de Documentos Públicos Extranjeros[39], hecho en La Haya el 5 de octubre de 1961, para sustituir las prescripciones vigentes por una forma simplificada y normalizada (la "apostilla"), que se utiliza para proporcionar la certificación de determinados documentos públicos en los Estados parte en el Convenio[40]. Únicamente una "autoridad competente" designada por el Estado del que emana el documento público puede expedir una apostilla. Las apostillas certifican la autenticidad de la firma, la calidad en que ha actuado la persona firmante del documento y, cuando proceda, la identidad del sello o timbre que lleva el documento, pero no se refieren al contenido del propio documento subyacente.

14. Como ya se ha indicado anteriormente, en muchos ordenamientos jurídicos no es necesario que los contratos comerciales figuren siempre en un documento o queden probados por escrito para que sean válidos. Incluso cuando existe un escrito, no es necesariamente obligatoria una firma para que el contrato sea vinculante para las partes. Por supuesto, cuando la ley exige que los contratos consten por escrito o estén firmados, el incumplimiento de esas prescripciones los anularía. Los requisitos de forma a efectos probatorios tal vez revistan más importancia que los requisitos de forma a efectos de la validez de los contratos. La dificultad de demostrar acuerdos orales es una de las principales razones por las que los contratos comerciales se recogen en documentos escritos o se documentan por correspondencia, incluso aunque un acuerdo oral fuera válido de otro modo. Es poco probable que las partes cuyas obligaciones están documentadas en escritos firmados logren negar el contenido de sus obligaciones. La aplicación de normas estrictas sobre pruebas documentales suele orientarse a aportar un alto grado de fiabilidad a los documentos que cumplen esas normas, lo que, según la opinión general, aumenta la certidumbre jurídica. Al mismo tiempo, no obstante, cuanto más complicados sean los requisitos probatorios, tanto mayor será la oportunidad que tienen las partes de invocar defectos de forma con miras a anular la validez o negar la fuerza ejecutiva de obligaciones que ya no tienen intención de cumplir, por ejemplo, porque el contrato ha resultado comercialmente desfavorable. Por lo tanto, es preciso equilibrar el interés por fomentar la seguridad en el intercambio de comunicaciones electrónicas con el riesgo de facilitar un método simple para que los comerciantes de mala fe repudien sus obligaciones legales libremente asumidas. La consecución de este equilibrio mediante normas y criterios que sean reconocidos internacionalmente y aplicables con carácter transfronterizo es una de las tareas principales de la actividad normativa en la esfera del comercio electrónico. El presente documento se propone ayudar a los legisladores y los encargados de formular políticas a identificar las principales cuestiones jurídicas que intervienen en la utilización internacional de métodos de autenticación y firma electrónicas y considerar posibles soluciones al respecto.

[39] Naciones Unidas, *Treaty Series*, vol. 527, Nº 7625.

[40] Entre esos documentos figuran los que emanan de una autoridad o funcionario relacionado con un juzgado o tribunal del Estado (incluidos los documentos expedidos por un tribunal administrativo, constitucional o eclesiástico, un fiscal, un secretario o un agente judicial); documentos administrativos; actas notariales; y certificados oficiales que se agregan en documentos firmados por personas a título personal.

Primera parte

Métodos de firma y autenticación electrónicas

Índice

I. Definición y métodos de firma y autenticación electrónicas

A. Observaciones generales sobre terminología

15. Las expresiones "autenticación electrónica" o "firma electrónica" se refieren a diversas técnicas existentes actualmente en el mercado o aún en fase de desarrollo destinadas a reproducir en un entorno electrónico algunas de las funciones, o todas ellas, señaladas como características de las firmas manuscritas o de otros métodos tradicionales de autenticación.

16. En el curso de los años se ha creado una serie de distintas técnicas de firma electrónica. Cada una de ellas tiene por objetivo atender a distintas necesidades y proporcionar distintos niveles de seguridad y también entraña diferentes requisitos técnicos. Los métodos de autenticación y firma electrónicas pueden clasificarse en tres categorías, a saber: los que se basan en lo que el usuario o el receptor sabe (por ejemplo, contraseñas, números de identificación personal (NIP)), los basados en las características físicas del usuario (por ejemplo, biométrica) y los que se fundamentan en la posesión de un objeto por el usuario (por ejemplo, códigos u otra información almacenados en una tarjeta magnética[41]. En una cuarta categoría se podría incluir a diversos tipos de métodos de autenticación y firma que, sin pertenecer a ninguna de las categorías arriba citadas, podrían también utilizarse para indicar el iniciador de una comunicación electrónica (por ejemplo, un facsímil de una firma manuscrita, o un nombre mecanografiado en la parte inferior de un mensaje electrónico). Entre las tecnologías que se utilizan en la actualidad figuran las firmas digitales en el marco de una infraestructura de clave pública (ICP), dispositivos biométricos, NIP, contraseñas elegidas por el usuario o asignadas, firmas manuscritas escaneadas, firmas realizadas por medio de un lápiz digital, y botones de pulsación del tipo de "sí" o "aceptar" o "acepto"[42]. Las soluciones híbridas basadas en la combinación de distintas tecnologías están adquiriendo una aceptación creciente, como por ejemplo en el caso del uso combinado de contraseñas y sistemas TLS/SSL (seguridad del estrato de transporte/estrato de zócalos seguro), que es una tecnología en la que se utiliza una combinación de cifrados de clave pública y simétrica. Las características de las principales técnicas de uso actual se describen infra (véanse los párrs. 25 a 66).

17. Como suele ocurrir, la tecnología apareció mucho antes de que el derecho se adentrara en este ámbito. El consiguiente desfase entre el derecho y la tecnología da

[41] Véase el informe del Grupo de Trabajo sobre Comercio Electrónico acerca de la labor de su 32º período de sesiones, celebrado en Viena del 19 al 30 de enero de 1998 (A/CN.9/446, párrs. 91 y sigs.).

[42] Ley Modelo de la CNUDMI sobre Firmas Electrónicas…, segunda parte, párr. 33.

pie no sólo a que existan distintos niveles de conocimientos especializados, sino también a una utilización contradictoria de la terminología. Se comenzó a utilizar expresiones que se habían empleado tradicionalmente con un matiz concreto en los ordenamientos jurídicos nacionales para describir técnicas electrónicas cuya funcionalidad no coincidía necesariamente con las funciones o las características del concepto correspondiente en el uso jurídico. Como ya se ha visto supra (véanse los párrs. 7 a 10), si bien es cierto que las nociones de "autenticación", "autenticidad", "firma" e "identidad" guardan estrecha relación en determinados contextos, no son idénticas ni intercambiables. Ahora bien, el uso en el sector de la tecnología de la información, que evolucionó básicamente alrededor de preocupaciones por la seguridad de las redes, no es forzosamente aplicable a las mismas categorías que los textos jurídicos.

18. En algunos casos, se emplea la expresión "autenticación electrónica" para referirse a unas técnicas que, según el contexto en que se utilicen, pueden suponer varios elementos, como la identificación de personas, la confirmación de la autoridad de una persona (por lo general para actuar en nombre de otra persona o entidad) o sus prerrogativas (por ejemplo, la pertenencia a una institución o su suscripción a un servicio) o una garantía sobre la integridad de la información. En algunos casos, se refiere únicamente a la identidad[43], aunque a veces se hace extensiva a la autoridad[44], o en una combinación de cualquiera de esos elementos o de todos ellos[45].

19. La Ley Modelo de la CNUDMI sobre Comercio Electrónico[46] y la Ley Modelo de la CNUDMI sobre Firmas Electrónicas[47] no utilizan la expresión "autenticación electrónica", habida cuenta del diferente significado de "autenticación" en diversos ordenamientos jurídicos y la posible confusión con procedimientos o requisitos de forma concretos. La Ley Modelo sobre Comercio Electrónico utiliza en cambio la noción de "forma original" para aportar los criterios de la equivalencia funcional de la

[43] La Administración de Tecnología del Departamento de Comercio de los Estados Unidos, por ejemplo, define la autenticación electrónica de la siguiente manera: "el proceso de determinar la confianza en las identidades de usuarios presentadas electrónicamente a un sistema de información" (Estados Unidos, Departamento de Comercio, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-63, versión 1.0.2 (Gaithersburg, Maryland, abril de 2006)), disponible en http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf (consultado el 5 de junio de 2008).

[44] Por ejemplo, el Gobierno de Australia creó un marco de autenticación electrónica en el que ésta se define como "el proceso de crear un nivel de confianza en que una declaración sea auténtica o válida al llevar a cabo una operación en línea o por teléfono. Ayuda a crear confianza en una operación en línea al ofrecer a las partes interesadas ciertas garantías de que sus tratos son legítimos. Entre esas declaraciones pueden figurar detalles sobre la identidad, títulos profesionales, o la autoridad delegada para realizar operaciones" (Australia, Departamento de Hacienda y Administración, *Australian Goverment e-Authentication Framework: An Overview* (Commonwealth de Australia, 2005), disponible en http://www.agimo.gov.au/infraestructure/authentication/agaf_b/overview/introduction#e-authentication (consultado el 5 de junio de 2008).

[45] En los Principios para la autenticación electrónica preparados por el Gobierno del Canadá, por ejemplo, se define la "autenticación" como "un proceso que da fe de los atributos de los participantes en una comunicación electrónica o de la integridad de la comunicación". A su vez, la definición de "atributos" es "la información relativa a la identidad, el privilegio o los derechos de un participante u otra entidad autenticada" (Canadá Industry Canada, *Principles for Electronic Authentication: a Canadian Framework* (Ottawa, mayo de 2004), disponible en http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html (consultado el 5 de junio de 2008).

[46] Ley Modelo de la CNUDMI sobre Comercio Electrónico ...

[47] Ley Modelo de la CNUDMI sobre Firmas Electrónicas ...

información electrónica "auténtica". Según el artículo 8 de la Ley Modelo, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:

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

b) De requerirse que la información sea presentada, si dicha información "puede ser mostrada a la persona a la que se deba presentar".

20. En consonancia con la distinción que la mayoría de ordenamientos jurídicos establecen entre firma (o sellos, cuando se utilizan en lugar de ésta) como medio de "autenticación", por una parte, y "autenticidad" como la calidad de un documento o de una información consignada, por la otra, ambas leyes modelo complementan la noción de "originalidad" con la noción de "firma". El apartado *a)* del artículo 2 de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas define la firma electrónica como los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para "identificar al firmante" en relación con el mensaje de datos y para "indicar que el firmante aprueba la información recogida en el mensaje de datos".

21. La definición de "firma electrónica" en los textos de la CNUDMI es deliberadamente amplia, para que abarque todos los métodos de "firma electrónica" existentes o futuros. Siempre que el método utilizado "es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos,"[48] a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente, se deberá considerar que cumplen las prescripciones legales en materia de firma. Los textos de la CNUDMI relativos al comercio electrónico, así como un gran número de otros textos legislativos, se basan en el principio de la neutralidad tecnológica y por lo tanto pretenden dar cabida a todas las formas de firma electrónica. Así pues, la definición de firma electrónica dada por la CNUDMI abarcaría todo el abanico de técnicas de "firma electrónica", desde los altos niveles de seguridad, como los sistemas de garantía de la firma basados en criptografía asociados a un sistema de ICP (una forma habitual de "firma digital" (véanse los párrs. 25 a 53), hasta los niveles de seguridad más bajos, como códigos o contraseñas no cifrados. La mera inclusión del nombre mecanografiado del autor al final de un mensaje de correo electrónico, que es la forma más habitual de "firma" electrónica, por ejemplo, cumpliría la función de identificar correctamente al autor del mensaje siempre que no sea infundado utilizar un nivel tan bajo de seguridad.

22. Las leyes modelo de la CNUDMI no se ocupan por otra parte de cuestiones relacionadas con el control del acceso o la verificación de la identidad. Esta circunstancia se ajustaba también al hecho de que, en un entorno basado en papel, las firmas podrán ser signos de identidad, pero son forzosamente atributos de identidad. La Ley Modelo de la CNUDMI sobre Comercio Electrónico se ocupa, no obstante, de las condiciones en que el destinatario de un mensaje de datos tendrá derecho a

[48] Ley Modelo de la CNUDMI sobre Comercio Electrónico …, artículo 7, apartado *b)* del párrafo 1.

considerar que el mensaje proviene efectivamente de su supuesto iniciador. De hecho, el artículo 13 de la Ley Modelo dispone que, en las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado: por alguna persona "facultada para actuar en nombre del iniciador respecto de ese mensaje"; o por "un sistema de información programado por el iniciador o en su nombre para que opere automáticamente". En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un mensaje de datos proviene del iniciador, y actuar en consecuencia, cuando *a)* para comprobar que el mensaje de datos provenía del iniciador, "el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin"; o *b)* el mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio. En conjunto, estas normas permiten que una parte deduzca la identidad de otra persona, tanto si el mensaje estaba "firmado" electrónicamente o no lo estaba, y si el método utilizado para atribuir el mensaje al iniciador se podía utilizar válidamente para fines de "firma" o no. Esto concuerda con la práctica vigente en el entorno basado en papel. Verificar la voz, el aspecto físico o los documentos de identidad (por ejemplo, un pasaporte nacional) de otra persona puede bastar para sacar la conclusión de que la persona es quien afirma ser a los efectos de comunicarse con la persona interesada, pero no se consideraría como "firma" de esa persona en el marco de la mayoría de ordenamientos jurídicos.

23. Aparte de la confusión que se ha producido por el hecho de que el uso técnico de expresiones en el entorno basado en papel y en el electrónico no coincide con el uso jurídico, las diversas técnicas mencionadas anteriormente (véase supra, párr. 16 y el análisis más detallado en los párrs. 24 a 66 *infra*) pueden utilizarse con fines diferentes y aportan una funcionalidad diferente, según el contexto. Pueden utilizarse contraseñas o códigos, por ejemplo, para "firmar" un documento electrónico, pero también se podrán emplear para obtener acceso a una red, a una base de datos o a otro servicio electrónico, igual que una llave se puede utilizar para abrir una caja fuerte o una puerta. Ahora bien, mientras que en el primer caso la contraseña es una prueba de identidad, en el segundo es una credencial o signo de autoridad que, aunque esté vinculada corrientemente a una persona concreta, también es susceptible de ser transferida a otra. En el caso de las firmas digitales, es incluso más patente que la terminología actual no es apropiada. La firma digital se considera una tecnología concreta para "firmar" documentos electrónicos. No obstante, como mínimo puede ponerse en duda que, desde un punto de vista jurídico, la aplicación de la criptografía asimétrica con fines de autenticación se califique como "firma" digital, ya que sus funciones trascienden de las funciones típicas de una firma manuscrita. La firma digital ofrece medios para "verificar la autenticidad de mensajes electrónicos" así como de "garantizar la integridad de su contenido". Además, la tecnología de la firma digital "no determina simplemente el origen o la integridad respecto de personas como es necesario a efectos de firma, sino que también puede autenticar, por ejemplo, servidores, sitios de Internet, programas informáticos, o cualesquiera otros datos que se distribuyan o almacenen de forma digital", lo que

confiere a las firmas digitales "una utilización mucho más amplia que la de alternativa electrónica de las firmas manuscritas"[49].

B. Principales métodos de firma y autenticación electrónicas

24. A los efectos del presente análisis se examinarán cuatro métodos principales de firma y autenticación: las firmas digitales; los métodos biométricos; las contraseñas y los métodos híbridos; y las firmas escaneadas o mecanografiadas.

1. Firmas digitales basadas en la criptografía de clave pública

25. Se entiende por "firma digital" la que se obtiene mediante aplicaciones tecnológicas en que se utiliza criptografía asimétrica, también denominada sistemas de cifrado de clave pública, para asegurar la autenticidad de los mensajes electrónicos y garantizar la integridad de su contenido. La firma digital se presenta de muchas formas distintas, por ejemplo, firmas digitales infalsificables, firmas ciegas y firmas digitales irrefutables.

a) Conceptos técnicos y terminología

i) *Criptografía*

26. Las firmas digitales se crean y verifican utilizando criptografía, rama de las matemáticas aplicadas que se ocupa de trasformar mensajes en formas aparentemente ininteligibles y se devuelven luego a su forma original. En las firmas digitales se utiliza lo que se denomina criptografía de clave pública, que se suele basar en el empleo de funciones algorítmicas para generar dos "claves" diferentes pero matemáticamente interrelacionadas (por ejemplo, grandes números producidos mediante una serie de fórmulas matemáticas aplicadas a números primos)[50]. Una de esas claves se utiliza para crear una firma digital o transformar datos en una forma en apariencia ininteligible, y la otra para verificar una firma digital o devolver el mensaje a su forma original[51]. El

[49] Babette Aalberts y Simone van der Hof, *Digital Signature Blindness: Analysis of Legislative Approaches toward Electronic Authentication* (noviembre de 1999), pág. 8, disponible en http://rechten.uvt.nl/simone/Digsigbl.pdf (consultado el 5 de junio de 2008).

[50] Cabe señalar, sin embargo, que el concepto de criptografía de clave pública que se examina aquí no implica necesariamente el empleo de algoritmos basados en números primos. En la actualidad se utilizan o se preparan otras técnicas matemáticas, como los criptosistemas de curvas elípticas, a los que suele atribuirse la posibilidad de ofrecer un alto grado de seguridad mediante el empleo de longitudes de clave considerablemente reducidas.

[51] Aunque el empleo de la criptografía es una de las principales características de las firmas digitales, el mero hecho de que éstas se utilicen para autenticar un mensaje que contenga información en forma digital no debe confundirse con el uso más e la criptografía con fines de confidencialidad. El cifrado con fines de confidencialidad es un método utilizado para codificar una comunicación electrónica de tal modo que sólo puedan leerla el iniciador y el destinatario del mensaje. En varios países la ley limita, por razones de orden público que pueden incluir consideraciones de defensa nacional, el empleo de criptografía con fines de confidencialidad. Sin embargo, el empleo a efectos de autenticación produciendo una firma digital no implica necesariamente que se utilice la criptografía para dar carácter confidencial a la información durante el proceso de comunicación, porque la firma digital cifrada puede sencillamente añadirse a un mensaje no cifrado.

equipo y los programas informáticos que utilizan dos de esas claves se suelen denominar en conjunto "criptosistemas" o, más concretamente, "criptosistemas asimétricos" cuando se basan en el empleo de algoritmos asimétricos.

ii) *Claves públicas y privadas*

27. Se denomina "clave privada" a una clave complementaria con que se producen firmas digitales, que utiliza únicamente el firmante para crear la firma digital y debe mantenerse en secreto, mientras que la "clave pública", es conocida de ordinario por más personas y la utiliza la parte que confía para verificar la firma digital. La clave privada puede mantenerse en una tarjeta con memoria, o es posible acceder a ella mediante un número de identificación personal (NIP) o un dispositivo de identificación biométrica, por ejemplo, mediante el reconocimiento de una huella dactilar. En caso de que muchas personas tengan que verificar la firma digital del firmante, la clave pública debe ponerse a disposición de todas o distribuirse entre ellas, por ejemplo, adjuntando los certificados a las firmas o utilizando otros medios para asegurar que las partes que confían, y únicamente las que deben verificar la firma, puedan obtener los certificados conexos. Aunque las claves del par están matemáticamente relacionadas entre sí, si un criptosistema asimétrico se ha concebido y aplicado en forma segura es virtualmente imposible deducir la clave privada partiendo de una clave pública conocida. Los algoritmos más comunes para el cifrado mediante las claves públicas y privadas se basan en una característica importante de los grandes números primos, a saber: una vez que se multiplican uno por otro para obtener un nuevo número, resulta especialmente difícil y laborioso determinar cuáles fueron los dos números primos que crearon ese nuevo gran número[52]. De este modo, aunque muchas personas conozcan la clave pública de un determinado firmante y puedan utilizarla para verificar su firma, no pueden descubrir la clave privada de ese firmante ni utilizarla para falsificar firmas digitales.

iii) *Función de control*

28. Además de la creación de pares de claves se utiliza otro proceso fundamental, que suele denominarse "función de control", para crear y verificar una firma digital. La función de control es un proceso matemático, basado en un algoritmo que crea una representación digital o forma comprimida del mensaje (llamada con frecuencia "compendio del mensaje" o "huella dactilar" del mensaje) como "valor de control"

[52] Algunas de las normas existentes aplican el concepto de "inviabilidad computacional" para referirse a la prevista irreversibilidad del procedimiento, es decir, la expectativa de que sea imposible deducir la clave privada secreta del usuario a partir de su clave pública. "La inviabilidad computacional es un concepto relativo que se basa en el valor de los datos protegidos, el volumen de las operaciones informáticas previas necesario para protegerlos, el período durante el cual requieren protección y el costo y el tiempo necesarios para atacar dichos datos, factores que se evalúan en la perspectiva actual y en la de los futuros avances tecnológicos". (Asociación de Abogados de los Estados Unidos, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (Chicago, Asociación de Abogados de los Estados Unidos, 1º de agosto de 1996, pág. 9, nota 23, disponible en http://www.abanet.org/scitech/ec/isc/dsgfree.html (consultado el 4 de junio de 2008)).

o "resultado de control" de una longitud estándar que suele ser mucho menor que la del mensaje pero que sin embargo corresponde en lo esencial exclusivamente a éste. Todo cambio en el mensaje produce invariablemente un resultado de control diferente cuando se utiliza la misma función de control. En el caso de una función de control segura, a la que se denomina en ocasiones "función de control unidireccional", es prácticamente imposible deducir el mensaje inicial aunque se conozca su valor de control. Otra característica básica de las funciones de control es que también resulta casi imposible encontrar otro objeto binario (es decir, distinto del utilizado en un principio para obtener el compendio) que produzca el mismo compendio. Por ello, las funciones de control permiten que los programas informáticos de creación de firmas digitales funcionen con cantidades de datos más pequeñas y predecibles y proporcionen al mismo tiempo una sólida correlación probatoria con el contenido del mensaje inicial y así dar eficientemente garantías de que el mensaje no se haya modificado después de haberse firmado digitalmente.

iv) *Creación de una firma digital*

29. Para firmar un documento o cualquier otro elemento de información, en primer lugar el firmante delimita con exactitud los márgenes dentro de los cuales estará contenida la información que se ha de firmar. Acto seguido, una función de control del programa informático del firmante calcula un resultado de control que (a todos los efectos prácticos) corresponde exclusivamente a la información que se ha de firmar. Ese mismo programa informático transforma luego el resultado de control en una firma digital utilizando la clave privada del firmante. Así pues, la firma digital resultante corresponde exclusivamente a la información que se firma y a la clave privada utilizada para crear dicha firma digital. Generalmente, la firma digital (el cifrado del resultado de control del mensaje con la clave privada del firmante) se adjunta al mensaje y se almacena o transmite junto con él. Sin embargo, también puede enviarse o almacenarse como elemento de datos independiente, siempre que mantenga una vinculación fiable con el mensaje correspondiente. Como la firma digital corresponde exclusivamente a su mensaje, es inservible si se disocia permanentemente de éste.

v) *Verificación de la firma digital*

30. La verificación de la firma digital es el procedimiento con que se comprueba esa firma por remisión al mensaje original y a una clave pública dada, determinando de esta forma si la firma digital fue creada para ese mismo mensaje utilizando la clave privada que corresponde a la clave pública remitida. La verificación de una firma digital se efectúa calculando un nuevo resultado de control del mensaje original mediante la misma función de control utilizada para crear la firma digital. Seguidamente, utilizando la clave pública y el nuevo resultado de control, el verificador comprueba si la firma digital se creó utilizando la clave privada correspondiente y si el nuevo resultado de control calculado corresponde al resultado de control original que fue transformado en la firma digital durante el trámite de firma.

31. El programa de verificación confirmará que la firma digital ha sido "verificada" desde el punto de vista criptográfico: *a)* si se utilizó la clave privada del firmante para firmar digitalmente el mensaje, cosa que se reconocerá si se ha utilizado la clave pública del firmante para verificar la firma, dado que esta clave pública sólo verificará una firma digital creada con la clave privada del firmante; y *b)* si el mensaje no se ha modificado, lo que se reconocerá si el resultado de control calculado por el verificador es idéntico al extraído de la firma digital durante el procedimiento de verificación.

vi) *Otros usos de las tecnología de firma digital*

32. La tecnología de firma digital sirve para mucho más que meramente "firmar" comunicaciones electrónicas del mismo modo en que se utiliza la firma manuscrita para refrendar documentos. Ciertamente, a menudo se utilizan, por ejemplo, certificados firmados digitalmente para "autenticar" servidores o sitios web, entre otras cosas, a fin de garantizar a sus usuarios que son lo que dicen ser o están efectivamente vinculados a la empresa que asegura administrarlos. La tecnología de firma digital puede utilizarse también para "autenticar", por ejemplo, programas informáticos con el fin de garantizar la autenticidad de los que se hayan descargado de un sitio web, para corroborar que un determinado servidor utiliza una tecnología generalmente reconocida por un cierto nivel de seguridad de la conexión, o para "autenticar" cualquier otro tipo de datos que se distribuyan o almacenen digitalmente.

b) Infraestructura de clave pública y prestadores de servicios de certificación

33. Para verificar una firma digital, el verificador debe tener acceso a la clave pública del firmante y tener la seguridad de que corresponde a su clave privada. Sin embargo, un par de claves pública y privada no tiene vinculación intrínseca con nadie; es simplemente un par de números. Se necesita otro mecanismo para vincular en forma fiable a una persona o entidad determinada con el par de claves. Ello es especialmente importante, porque tal vez no haya relación de confianza anterior entre el firmante y los destinatarios de las comunicaciones firmadas digitalmente. A tal efecto, las partes interesadas deben tener cierto grado de confianza en las claves pública y privada que se expidan.

34. Puede que exista el nivel de confianza requerido entre partes que confíen unas en otras, que se hayan tratado durante algún tiempo, que se comuniquen mediante sistemas cerrados, que actúen dentro de un grupo cerrado, o que puedan regir sus operaciones en base a un contrato, por ejemplo, en un acuerdo de asociación comercial. En una operación en la que participen sólo dos partes, cada una puede sencillamente comunicar (por un conducto relativamente seguro, como un servicio de mensajería o por teléfono) la clave pública del par de claves que cada parte utilizará. Sin embargo, este nivel de confianza puede no existir entre partes que se relacionen con poca frecuencia, que se comuniquen a través de sistemas abiertos (por ejemplo, Internet), que no formen parte de un grupo cerrado o que no tengan acuerdos de asociación comercial

u otros acuerdos que rijan sus relaciones. Además, cabe tener presente que, en caso de que deban resolverse controversias en los tribunales o mediante arbitraje, puede resultar difícil demostrar si el dueño legítimo de una determinada clave pública la ha revelado o no al destinatario.

35. Un posible firmante podría hacer una declaración pública indicando que debe considerarse que las firmas verificables por una clave pública determinada proceden de él. La forma y la eficacia jurídica de esa declaración se regirían por la ley del Estado promulgador. Por ejemplo, la presunción de que una firma electrónica corresponde a un determinado firmante podría corroborarse con la publicación de la declaración en un boletín oficial o un documento de "autenticidad" reconocida por las autoridades públicas. Sin embargo, es posible que otras partes no estén dispuestas a aceptar la declaración, especialmente si no hay contrato previo que establezca con certeza el efecto jurídico de esa declaración publicada. La parte que se base en esa declaración publicada sin respaldo en un sistema abierto correría el gran riesgo de confiar inadvertidamente en un impostor, o de tener que impugnar el desconocimiento fraudulento de una firma digital (cuestión a menudo mencionada en el contexto del "repudio negativo" de firmas digitales) si la operación resulta desfavorable para el supuesto firmante.

36. Una forma de resolver algunos de estos problemas es recurrir a uno o más terceros para vincular a un firmante identificado o su nombre con una clave pública determinada. El tercero se conoce en general, en la mayoría de las normas y directrices técnicas, como "autoridad certificadora", "prestador de servicios de certificación" o "proveedor de servicios de certificación" (en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas se ha elegido el término "prestador de servicios de certificación"). En algunos países, esas autoridades certificadoras se han ido organizando jerárquicamente, en lo que suele denominarse infraestructura de clave pública (ICP). Las autoridades certificadoras de una ICP pueden establecerse conforme a una estructura jerárquica en la que algunas certifican únicamente a otras que prestan servicios directamente a los usuarios. En tal estructura, algunas autoridades certificadoras quedan subordinadas a otras. En otras formas concebibles de organizarlas, todas ellas pueden funcionar en pie de igualdad. En toda ICP de gran tamaño podría haber entidades de certificación subordinadas y superiores. Entre otras soluciones cabe citar, por ejemplo, la expedición de certificados por las partes que confían.

i) *Infraestructura de clave pública*

37. Establecer una ICP es una forma de crear confianza en que: *a)* la clave pública del usuario no ha sido alterada y corresponde efectivamente a la clave privada del mismo usuario; y *b)* se han utilizado buenas técnicas criptográficas. Para crear la confianza señalada más arriba, una ICP puede prestar diversos servicios, como los siguientes: *a)* gestión de las claves criptográficas utilizadas para las firmas digitales; *b)* certificación de que una clave pública corresponde a una clave privada; *c)* suministro de claves a usuarios finales; *d)* publicación de información sobre la revocación de claves públicas o certificadas; *e)* administración de símbolos personales (por ejemplo, tarjetas con memoria) que permitan identificar al usuario con información de identificación

personal exclusiva o que permitan generar y almacenar claves privadas individuales; *f)* comprobación de la identificación de los usuarios finales y prestación de servicios a éstos; *g)* prestación de servicios de marcado cronológico; y *h)* gestión de las claves criptográficas utilizadas con fines de confidencialidad en los casos en que se autorice el empleo de esa técnica.

38. Una ICP suele basarse en diversos niveles jerárquicos de autoridad. Por ejemplo, los modelos considerados en ciertos países para establecer una posible ICP entrañan referencias a los siguientes niveles: *a)* una "autoridad principal" única que certificaría la tecnología y las prácticas de todas las partes autorizadas para expedir pares de claves o certificados criptográficos en relación con el empleo de dichos pares de claves, y llevaría un registro de las autoridades de certificación subordinadas[53]; *b)* diversas autoridades de certificación, subordinadas a la "principal", que certificarían que la clave pública de un usuario corresponde en realidad a la clave privada del mismo usuario (es decir, que no ha sido objeto de manipulación indebida); y *c)* diversas entidades locales de registro, subordinadas a las autoridades de certificación, que recibirían de los usuarios peticiones de pares de claves criptográficas o de certificados relativos al empleo de esos pares de claves, exigirían pruebas de identidad a los posibles usuarios y las verificarían. En ciertos países se prevé que los notarios podrían actuar como autoridades locales de registro o prestar apoyo a dichas autoridades.

39. Las ICP organizadas en una estructura jerárquica pueden ampliarse en el sentido de que es posible que incorporen "colectividades" enteras de nuevas ICP, por el mero expediente de que la "autoridad principal" establezca una relación de confianza con la "autoridad principal" de la nueva colectividad[54]. La autoridad principal de la nueva colectividad puede incorporarse directamente en régimen de sujeción a la autoridad principal de la ICP receptora, subordinándose a ella. La autoridad principal de la nueva colectividad podrá convertirse también en prestador de servicios de certificación subordinado de otro de los prestadores de servicios de certificación subordinados de la ICP existente. Otro aspecto interesante de las ICP jerarquizadas es que resulta fácil establecer el historial de certificación, porque éste va en una sola dirección, retrospectivamente desde el certificado del usuario hasta el momento en que éste elige una entidad en que confiar. Además, el historial de certificación en una ICP jerarquizada es relativamente breve, y los usuarios de un sistema jerarquizado saben implícitamente para qué aplicaciones sirve un certificado, según la posición que ocupe el prestador de servicios de certificación en esa jerarquía. Sin embargo, las ICP jerarquizadas también tienen desventajas, principalmente porque se basan en la confianza depositada en una sola de ellas. Si la autoridad principal se ve comprometida, ello afecta a toda la ICP. Además, en algunos países ha resultado difícil elegir una sola entidad como autoridad principal e imponer esta jerarquía a todos los demás prestadores de servicios de certificación[55].

---

[53] La cuestión de si un gobierno debe tener capacidad técnica para conservar o recrear claves de confidencialidad privada podría abordarse a nivel de las autoridades principales.

[54] William T. Polk y Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructure*, National Institute of Standards and Technology (septiembre de 2000), disponible en http://csrc.nist.gov/pki/documents/B2B-article.pdf (consultado el 5 de junio de 2008).

[55] Polk y Hastings, (*Bridge Certification Authorities…*) señalan que en los Estados Unidos de América, fue muy difícil elegir al organismo del Gobierno federal que asumiría la autoridad general respecto de la ICP federal.

40. La llamada ICP "en malla" es una opción ante la ICP jerarquizada. Conforme a este modelo, los prestadores de servicios de certificación forman parte de una relación entre iguales. Cualquiera de los que actúan conforme a este modelo puede ser el depositario de la confianza. Por regla general, el usuario confía en el que expidió su certificado. Los prestadores de servicios de certificación podrán expedirse recíprocamente certificados; este par de certificados refleja su relación de confianza mutua. La ausencia de jerarquía en este sistema significa que los prestadores de servicios de certificación no pueden imponer condiciones que rijan los tipos de certificados expedidos por otros prestadores de dichos servicios. Si uno de ellos desea limitar la confianza que se otorgue a otros, deberá indicar estas limitaciones en los certificados expedidos a sus colegas[56]. Sin embargo, armonizar las condiciones y las limitaciones de reconocimiento mutuo puede resultar sumamente complejo.

41. La tercera estructura opcional es la del prestador de servicios de certificación "intermedio". Esta estructura puede resultar especialmente útil para que varias colectividades de ICP anteriores confíen en sus respectivos certificados. A diferencia del prestador de servicios de certificación de una ICP "en malla", el "intermediario" no expide certificados directamente a los usuarios. No se prevé tampoco que este "intermediario" sea objeto de la confianza de los usuarios de la ICP, como sería el caso de un prestador de servicios de certificación "principal". En lugar de ello, el "intermediario" establece relaciones de confianza entre iguales con las distintas colectividades de usuarios, permitiendo de este modo que éstos conserven los depositarios naturales de su confianza en sus ICP respectivas. Si una colectividad de usuarios implanta un dominio de confianza en forma de una ICP jerarquizada, el prestador de servicios de certificación "intermedio" establece una relación con la autoridad principal de esa ICP. Sin embargo, si la colectividad de usuarios implanta un dominio de confianza creando una red de ICP, el prestador de servicios de certificación "intermedio" necesita únicamente entablar una relación con uno de los prestadores de servicios de certificación de la ICP, que pasa a ser el "principal" prestador de servicios de certificación de esa ICP a efectos de la "mediación de confianza" con la otra ICP. Esta "mediación de confianza", que une a dos o más ICP por su relación mutua con un prestador de servicios de certificación "intermedio" permite a los miembros de distintas colectividades de usuarios interactuar entre sí mediante el prestador de servicios de certificación "intermedio", con un grado de confianza determinado[57].

ii) *Prestador de servicios de certificación*

42. Para vincular un par de claves a un posible firmante, el prestador de servicios de certificación (o autoridad certificadora) expide un certificado, que es un registro electrónico en que se indica una clave pública junto con el nombre del suscriptor del certificado como "sujeto" del certificado, y con el que puede confirmarse que el

[56] Polk y Hastings, Bridge Certification Authorities…

[57] La estructura que se eligió en último término para establecer el sistema de ICP del Gobierno federal de los Estados Unidos fue la del prestador de servicios de certificación "intermedio" (Polk y Hastings, *Bridge Certification Autorities…*). El mismo modelo siguió el Gobierno del Japón para establecer su sistema de ICP.

firmante potencial que figura en el certificado posee la clave privada correspondiente. La función principal del certificado es vincular una clave pública a un firmante concreto. El "receptor" del certificado que desee confiar en la firma digital creada por el firmante que figura en él puede utilizar la clave pública indicada en ese certificado para verificar si la firma digital se creó con la clave privada correspondiente. Si dicha verificación es positiva, se obtiene técnicamente cierta garantía de que la firma digital fue creada por el firmante y de que la parte del mensaje utilizada en la función de control (y, por ello, el correspondiente mensaje de datos) no se ha modificado desde que se firmó digitalmente.

43. Para asegurar la autenticidad del certificado con respecto tanto a su contenido como a su fuente, el prestador de servicios de certificación lo firma en forma digital. La firma digital del prestador de servicios de certificación que figura en el certificado se puede verificar utilizando su clave pública, que figura en el certificado de otra entidad certificadora (que puede ser, aunque no necesariamente, de un nivel jerárquico superior) y ese otro certificado puede autenticarse a la vez utilizando la clave pública incluida en un tercer certificado, y así sucesivamente hasta que la persona que confíe en la firma digital tenga seguridad suficiente de su autenticidad. Entre otros métodos posibles para verificar la firma digital, esa firma se puede registrar en un certificado emitido por el prestador de servicios de certificación (que se denomina en ocasiones "certificado raíz")[58].

44. En todos los casos, el prestador de servicios de certificación que expida el certificado podrá firmarlo digitalmente durante el período de validez del otro certificado utilizado para verificar la firma digital del prestador de servicios de certificación. Para fomentar la confianza en la firma digital del prestador de servicios de certificación, algunos Estados prevén la publicación en un boletín oficial de la clave pública del prestador de servicios de certificación o de ciertos datos sobre el certificado raíz (como "huella dactilar").

45. La firma digital correspondiente a un mensaje, ya sea creada por el firmante para autenticar un mensaje o por un prestador de servicios de certificación para autenticar su certificado, deberá contener por lo general un sello cronológico fiable para que el verificador pueda determinar con certeza si la firma digital se creó durante el "período de validez" indicado en el certificado y, en cualquier caso, si el certificado era válido (es decir, no figuraba en una lista de los revocados) en el momento pertinente, que es una condición para poder verificar una firma digital.

46. Para que una clave pública y su correspondencia con un firmante determinado se puedan utilizar fácilmente en una verificación, el certificado podrá publicarse en un repertorio o difundirse por otros medios. Normalmente, estos repertorios son bases de datos en línea de certificados y de otro tipo de información a las que se puede acceder y que pueden utilizarse para verificar firmas digitales.

[58] Ley Modelo de la CNUDMI sobre Firmas Electrónicas…, segunda parte, párr. 54.

47. Una vez expedido, puede que un certificado no sea fiable, por ejemplo si el titular falsifica su identidad ante el prestador de servicios de certificación. En otros casos, un certificado puede ser suficientemente fiable cuando se expide pero deja de serlo posteriormente. Si la clave privada ha quedado "en entredicho", por ejemplo, si el firmante ha perdido el control de ésta, el certificado puede dejar de ser fiable y el prestador de servicios de certificación (a petición del firmante o aun sin su consentimiento, según las circunstancias), puede suspender (interrumpir temporalmente el período de validez) o revocar (invalidar de forma permanente) el certificado. Oportunamente después de suspender o revocar un certificado, cabe prever que el prestador de servicios de certificación haga pública la revocación o suspensión o notifique este hecho a las personas que soliciten información o de que se tenga conocimiento de que han recibido una firma digital verificable por remisión al certificado que carezca de fiabilidad. Del mismo modo, se debe examinar también, cuando proceda, si corresponde revocar el certificado del prestador de servicios, así como el certificado para verificar la firma de la entidad a cargo de la indicación cronológica en los vales que ésta expida y aquéllos de la entidad certificadora que hubiera expedido los certificados de dicha entidad encargada de la indicación cronológica.

48. La explotación de las autoridades certificadoras podría estar a cargo de prestadores de servicios del sector privado o de autoridades estatales. En algunos países, por razones de orden público, se prevé que sólo las entidades públicas estén autorizadas para actuar como autoridades certificadoras. Sin embargo, en la mayoría de los países los servicios de certificación se dejan totalmente en manos del sector privado, o los prestadores de servicios de certificación administrados por el Estado coexisten con los privados. Existen también sistemas de certificación cerrados, en los que establecen sus propios prestadores de servicios grupos pequeños. En algunos países los prestadores de servicios de certificación de propiedad estatal expiden certificados únicamente para respaldar firmas digitales utilizadas por la administración pública. Sean públicas o privadas estas autoridades certificadoras y deban o no obtener licencia para funcionar, normalmente hay más de una en la ICP. Plantea especial inquietud la relación entre ellas (véanse los párrafos 38 a 41 *supra*).

49. Puede que corresponda al prestador de servicios de certificación o a la autoridad principal asegurar que sus requisitos de política se cumplan de forma permanente. Aunque la elección de las autoridades certificadoras puede basarse en diversos factores, como la solidez de la clave pública utilizada y la identidad del usuario, la fiabilidad del prestador de servicios de certificación puede depender también de su observancia de las normas para expedir certificados y de la precisión con que evalúe los datos recibidos de los usuarios que soliciten certificados. Es de especial importancia el régimen de responsabilidad que se aplique al prestador de servicios de certificación con respecto al cumplimiento, en todo momento, de la política y los requisitos de seguridad de la autoridad principal o del prestador de servicios de certificación superior, o de cualquier otro requisito aplicable. Igualmente importante es la obligación del prestador de servicios de certificación de actuar conforme a las declaraciones que haya hecho sobre sus normas y prácticas, como se prevé en el apartado *a)* del párrafo 1 del artículo 9 de la Ley Modelo sobre Firmas Electrónicas.

c) Problemas prácticos para establecer la infraestructura de clave pública

50. Pese a los conocimientos considerables sobre las tecnologías de firma digital y su funcionamiento, para implantar en la práctica infraestructuras de clave pública y mecanismos de firma digital han surgido algunos problemas que han impedido utilizar la firma digital conforme a las expectativas.

51. La firma digital funciona bien como un medio para verificar las firmas que se crean durante el período de validez de un certificado. Sin embargo, cuando el certificado caduca o se revoca la clave pública correspondiente pierde validez, aunque no esté en entredicho el par de claves. Por ello, todo mecanismo de ICP requeriría un sistema de gestión de la firma digital para asegurar que la firma siga disponible a lo largo del tiempo. La dificultad principal proviene del riesgo de que los registros electrónicos "originales" (esto es, los dígitos binarios o "bitios" que conforman el fichero informático en que se registra la información), incluida la firma digital, pueden resultar ilegibles o poco fiables con el tiempo, principalmente por la obsolescencia del programa, del equipo físico o de ambos. De hecho, la firma digital podría resultar insegura por los avances científicos en materia de criptoanálisis; el programa de verificación de las firmas podría faltar durante períodos prolongados, o el documento podría perder su integridad[59]. Por ello, la conservación a largo plazo de la firma electrónica es en general problemática. Aunque por un tiempo se consideró que la firma digital era indispensable a efectos de archivo, la experiencia ha demostrado que no está exenta de riesgos a largo plazo. Como toda modificación del registro posterior al momento de creación de la firma dará lugar a que la verificación no funcione, las operaciones de reformateado destinadas a mantener la legibilidad futura del registro (como la "migración" o la "conversión") pueden afectar a la durabilidad de la firma[60]. En realidad, la firma digital se concibió más para dar seguridad a la comunicación de

[59] Jean-François Blanchette, "Defining electronic authenticity: an interdisciplinary journey", disponible en http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf (consultado el 5 de junio de 2008) (monografía publicada en un suplemento de las actas de la Conferencia internacional sobre sistemas y redes fiables, de 2004, celebrada en Florencia (Italia) del 28 de junio al 1º de julio de 2004, págs. 228 a 232).

[60] "En último término, los bitios es lo único que podemos preservar en un contexto electrónico. Sin embargo, desde hace tiempo está clara la gran dificultad de mantener indefinidamente una serie de bitios, ya que con el paso del tiempo se hace ilegible (para la computadora y, por consiguiente, para los seres humanos) debido a la obsolescencia tecnológica del programa de aplicación y del equipo informático (por ejemplo, el lector), o de ambos. Hasta ahora el problema de la duración de las firmas digitales basadas en la ICP se ha estudiado poco debido a su complejidad. ... Aunque las herramientas de autenticación utilizadas en el pasado, por ejemplo, las firmas manuscritas, los sellos, los timbres, las huellas dactilares, etc., también tienen que reformatearse (por ejemplo, microfilmándolas) debido a la obsolescencia del soporte de papel, una vez reformateadas nunca quedan inutilizadas por completo. Siempre existe como mínimo una copia disponible que puede compararse con otras herramientas de autenticación originales." (Jos Dumortier y Sofie Van den Eynde, *Electronic Signatures and Trusted Archival Services*, página 5, disponible en http://law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where (consultado el 5 de junio de 2008).

información que para conservarla[61]. Las iniciativas para superar este problema todavía no han dado con una solución duradera[62].

52. Otro ámbito en que las firmas digitales y los sistemas de ICP pueden plantear problemas prácticos es la seguridad de los datos y la protección de la esfera privada. Los prestadores de servicios de certificación deben mantener a buen recaudo las claves utilizadas para firmar los certificados que expidan a sus clientes, y podrán verse expuestos a tentativas de obtener acceso a las claves sin autorización (véase también la segunda parte, párrafos 223 a 226, *infra*). Además, los

[61] Los archiveros de varios países lanzaron en 1999 el proyecto titulado Investigación Internacional sobre los Registros Auténticos Permanentes de los Sistemas Electrónicos (InterPARES), con la finalidad de "desarrollar el conocimiento teórico y metodológico esencial para preservar durante largo tiempo los registros auténticos creados o mantenidos en forma digital, o ambas cosas a la vez" (véase http://www.interpares.org , consultado el 5 de junio de 2008). El proyecto de informe del Grupo de Trabajo Especial sobre autenticidad, disponible en http://www.interpares.org/documents/atf_draft_final_report.pdf (consultado el 5 de junio de 2008), que formó parte de la primera fase del proyecto (InterPARES 1, terminado en 2001), indicó que "las firmas digitales y las infraestructuras de clave pública (ICP) son ejemplos de tecnologías que se han desarrollado y aplicado como medio de autenticación de registros electrónicos que se transmiten a través del espacio. Aunque los registradores y el personal de tecnología de la información confían en las tecnologías de autenticación para garantizar la autenticidad de los registros, nunca se pretendió que estas tecnologías fuesen, y no lo son en la actualidad , un medio viable de garantizar la autenticidad de los registros electrónicos con el transcurso del tiempo" (destacamos este extremo). El informe final de InterPARES 1 está disponible en http://www.interpares.org/book/index.htm (consultado el 5 de junio de 2008). La continuación del proyecto (InterPARES 2) tiene por finalidad desarrollar y articular los conceptos, principios, criterios y métodos que puedan garantizar la creación y el mantenimiento de registros precisos y fidedignos y la preservación durante largo tiempo de registros auténticos en el contexto de las actividades artísticas, científicas y gubernamentales llevadas a cabo entre 1999 y 2001.

[62] Por ejemplo, la Iniciativa europea de normas para firmas electrónicas (EESSI), fue lanzada en 1999 por la Information and Communications Technology Standards Board, grupo de organizaciones colaboradoras que se ocupa de la normalización y actividades conexas en el ámbito de las tecnologías de la información y la comunicación, creado para coordinar las actividades en materia de normalización a fin de apoyar la aplicación de la Directiva de la Unión Europea sobre la firma electrónica (véase *Diario Oficial de las Comunidades Europeas*, L/13/12, 19 de enero de 2000). El consorcio de la EESSI (iniciativa de normalización con la que se procura incluir los requisitos de la directiva europea sobre la firma electrónica en las normas europeas) ha tratado de satisfacer la necesidad de asegurar la conservación a largo plazo de los documentos firmados criptográficamente, mediante su norma sobre el formato de firma electrónica (Electronic Signature Formats ES 201 733, ETSI 2000). En ese formato se distinguen los momentos de validación de la firma: la validación inicial y la validación posterior. El formato de ésta última abarca toda la información que puede utilizarse en su momento en el trámite de validación, como la relativa a la revocación, la indicación de fecha y hora, las políticas de firma, etc. Esta información se reúne en la etapa de validación inicial. Preocupaba a los creadores de estos formatos de firma electrónica el riesgo de seguridad para la validez de la firma debido a la degradación de la clave criptográfica. Como salvaguardia contra este riesgo de degradación, las firmas de la EESSI se estampan periódicamente con indicación de fecha y hora, ajustando los algoritmos de firma y el tamaño de la clave a los métodos modernos de análisis criptográfico. El problema de la longevidad de los programas informáticos se abordó en un informe de 2000 de la EESSI, en que se presentaron los "servicios de archivo fiables", ("trusted archival services"), un tipo nuevo de servicio comercial que prestarían órganos y gremios profesionales competentes aún no determinados para garantizar la conservación a largo plazo de los documentos firmados criptográficamente. En el informe se enumeran varios requisitos técnicos que deberían cumplir estos servicios de archivo, entre ellos la "retrocompatibilidad" con el equipo y los programas informáticos, mediante la conservación de este equipo o la emulación (véase Blanchette, "Defining electronic authenticity ..."). En el sitio http://www.law.kuleuven.ac.be/ icri/publications/91TAS-Report.pdf?where= (consultado el 5 de junio de 2008), figura un estudio de seguimiento de la recomendación de la EESSI acerca de los servicios de archivo fiables, realizado por el Centro interdisciplinario de derecho y tecnología de la información de la Universidad Católica de Lovaina (Bélgica), titulado *European Electronic Signature Standardization Initiative: Trusted Archival Services* (tercera fase, informe final, 28 de agosto de 2000). La EESSI se dio por terminada en octubre de 2004. No parece hallarse en funciones actualmente ningún sistema para aplicar estas recomendaciones (véase Dumortier y Van den Eynde, *Electronic Signatures and Trusted Archival Services…*).

prestadores de servicios de certificación tienen que obtener una serie de datos personales y comerciales de las personas que soliciten certificados, y archivarlos a efectos de consulta futura. También deben adoptar las medidas pertinentes para que el acceso a dicha información se ajuste a las leyes aplicables en materia de protección de datos[63]. No obstante, el acceso no autorizado a los datos sigue siendo una amenaza real.

2. Biométrica

53. La medición biométrica se utiliza para identificar a una persona por sus rasgos físicos o de comportamiento intrínsecos. Los rasgos que pueden utilizarse para el reconocimiento biométrico son el ADN, las huellas dactilares, el iris, la retina, la geometría de las manos o el rostro, el termograma facial, la forma de la oreja, la voz, el olor corporal, la configuración de los vasos sanguíneos, la letra, el modo de andar y la forma de mecanografiar.

54. La utilización de dispositivos biométricos supone por lo general captar una muestra biométrica, en forma digital, de algún rasgo biológico de una persona, y a continuación se extraen datos biométricos de esa muestra para crear una plantilla de referencia. Se confirma la identidad de la persona a la que pertenece la muestra biométrica, o se verifica la autenticidad de las comunicaciones presuntamente originadas por esa persona, comparando sus datos biométricos con los almacenados en la plantilla de referencia[64].

55. Algunos de los riesgos que se plantean guardan relación con el almacenamiento de los datos biométricos, porque las pautas biométricas son por lo general irrevocables. Si la integridad de los sistemas biométricos ha resultado comprometida, el usuario legítimo no tiene otra opción que la de revocar los datos de identificación y cambiarse a otro conjunto de datos de identificación intactos. Por ello, se necesitan reglas especiales para impedir el uso indebido de las bases de datos biométricas.

56. Las técnicas biométricas no pueden ser absolutamente exactas, pues los rasgos biológicos tienden a ser intrínsecamente variables, por lo que toda medición puede tener un margen de error. Al respecto, la biométrica no se considera un factor

[63] Véase Organización de Cooperación y Desarrollo Económicos (OCDE), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (París, 1980), disponible en http://www.oecd.org/document/18/0,2340,en_2649_34255_ 1815186_1_1_1_1,00.html (consultado el 5 de junio de 2008); Convenio para la protección de las personas en relación con el proceso automático de datos personales, del Consejo de Europa, *European Treaty Series*, Nº 108), disponible en http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (consultado en junio de 2008); Principios rectores sobre la utilización de ficheros computarizados de datos personales de las Naciones Unidas (resolución 45/95 de la Asamblea General); y Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (*Diario Oficial de las Comunidades Europeas*, L 281, de 23 de noviembre de 1995, disponible en http://eurlex.europa.eu/smartapi/cgi/sga_doc? smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett (consultado en junio de 2008).

[64] International Association for Biometrics e International Computer Security Association, *1999 Glossary of Biometric Terms* (copia disponible en la Secretaría).

identificador exclusivo, sino semiexclusivo. A fin de reflejar estas variaciones, puede manipularse la exactitud de la biométrica fijando un umbral de correlación para cotejar la plantilla de referencia con la muestra extraída. Sin embargo, un umbral bajo de correlación puede sesgar el ensayo induciendo una aceptabilidad falsa, mientras que uno elevado tal vez tienda a inducir rechazos erróneos. Sin embargo, la exactitud de la autenticación basada en métodos biométricos puede resultar apropiada en la mayoría de las aplicaciones comerciales.

57. Además, se plantean cuestiones relativas a la protección de los datos y los derechos humanos en lo tocante al almacenamiento y la divulgación de datos biométricos. Las leyes sobre protección de los datos[65], aunque no hagan referencia expresa a los sistemas biométricos, tienen por objeto proteger los datos personales de las personas físicas, cuyo procesamiento, a la vez en su forma primaria y como plantillas, es la base de la tecnología biométrica[66]. Además, tal vez se requieran medidas para proteger a los consumidores del riesgo de la utilización privada de datos biométricos y del eventual robo de identidad. Pueden entrar en juego también otros ámbitos jurídicos, como la legislación laboral y en materia de salud[67].

58. Los medios técnicos pueden ayudar a abordar algunas preocupaciones. Por ejemplo, el almacenamiento de datos biométricos en tarjetas o fichas con memoria puede salvaguardarlos de la posibilidad de acceso no autorizado si se almacenan en un sistema informático centralizado. Además, se han creado prácticas óptimas para reducir riesgos en distintos ámbitos, como el alcance y las capacidades; la protección de los datos; el control de los datos personales por el usuario; y la divulgación, auditoría, rendición de cuentas y supervisión[68].

59. Se considera en general que los dispositivos biométricos brindan un elevado grado de seguridad. Aunque resultan compatibles con una diversidad de usos, en la actualidad los utilizan principalmente los gobiernos, en particular los servicios de seguridad, por ejemplo, para permisos de inmigración y controles de acceso.

60. También se han elaborado aplicaciones comerciales, en que se utiliza con frecuencia la biométrica en el contexto de un procedimiento de autenticación basado en dos factores, que exige la presentación de un elemento biométrico que la persona tiene en su poder y otro que esa persona conoce (por lo general, una contraseña o un NIP). Además, se han creado aplicaciones para guardar en memoria y comparar las

---

[65] Véase la nota 63.

[66] Paul de Hert, *Biometrics: Legal Issues and Implications*, documento de antecedentes para el Instituto de Estudios Tecnológicos Prospectivos de la Comisión Europea (Centro Común de Investigación de la Dirección General de las Comunidades Europeas, 2005), pág. 13, disponible en http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf (consultado el 5 de junio de 2008).

[67] Por ejemplo, en el Canadá se examinó la utilización de la biométrica con respecto a la aplicación de la Ley de Protección de la Información Personal y Documentos Electrónicos (2000, cap. 5) en el lugar de trabajo (véase *Turner contra TELUS Communications Inc.*, 2005 FC 1601, 29 de noviembre de 2005 (Tribunal Federal del Canadá)).

[68] Como ejemplo de prácticas óptimas, véase la Iniciativa sobre bioprivacidad, "Best practices for privacy-sympathetic biometric deployment, del Grupo Biométrico Internacional, disponible en http://www.bioprivacy.org (consultado el 5 de junio de 2008).

características de una firma manuscrita. Se registra en tablillas digitales la presión de la pluma de escribir y el tiempo que se tarda en firmar. Los datos se almacenan luego en forma de algoritmo que servirá a efectos de comparación con firmas futuras. No obstante, por las características intrínsecas de la biométrica, se deben tener presentes los peligros del aumento gradual y descontrolado de su uso en operaciones comerciales corrientes.

61. Si se utiliza la firma biométrica como sustituto de la firma manuscrita, puede plantearse un problema en cuanto a la prueba. Como se señaló antes, la fiabilidad de la prueba biométrica varía según las tecnologías utilizadas y el margen aceptado de reconocimiento erróneo. Además, existe la posibilidad de que se manipulen indebidamente o se falsifiquen los datos biométricos memorizados en formato digital.

62. Pueden aplicarse a la utilización de firmas biométricas los mecanismos generales para verificar la fiabilidad previstos en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas y la Ley Modelo de la CNUDMI sobre Comercio Electrónico, así como en la más reciente Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales[69]. Para asegurar la uniformidad, también podría ser útil elaborar directrices internacionales sobre el uso y la gestión de métodos biométricos[70]. Debe estudiarse con atención si estas normas serían prematuras habida cuenta del grado de desarrollo actual de las tecnologías biométricas, y si ello no obstaculizaría el avance de éstas.

3. Contraseñas y métodos híbridos

63. Para controlar el acceso a información o servicios y para "firmar" comunicaciones electrónicas se utilizan contraseñas y códigos. En la práctica, este último uso es menos frecuente, por el riesgo de poner en entredicho el código si se transmite en mensajes no cifrados. Como fuere, las contraseñas y los códigos son el método de "autenticación" más utilizado a efectos del control del acceso y la verificación de la identidad en una diversidad de operaciones, incluidas casi todas las bancarias por Internet, la retirada de efectivo en cajeros automáticos y las compras con tarjeta de crédito.

64. Cabe reconocer que es posible utilizar muchas tecnologías para "autenticar" una operación electrónica. En una operación determinada pueden emplearse varias de ellas o diversas versiones de la misma. Por ejemplo, la dinámica de la firma a efectos de autenticación puede conjugarse con criptografía para ratificar la integridad del mensaje. Opcionalmente, pueden transmitirse contraseñas por Internet mediante criptografía (por ejemplo, SSL en los navegadores) para protegerlas, conjuntamente

[69] El proyecto de Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales fue adoptado por la CNUDMI en su 38º período de sesiones (Viena, 4 a 15 de julio de 2005). La Convención fue aprobada por la Asamblea General en virtud de su resolución 60/21, de 23 de noviembre de 2005.

[70] Estas directrices podrían compararse con los criterios de fiabilidad expuestos en la "Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas (*Ley Modelo de la CNUDMI sobre Firmas Electrónicas*…, segunda parte, párr. 75).

con la utilización de sistemas biométricos para crear una firma digital (criptografía asimétrica), que al recibirse genera un justificante de autenticación del protocolo Kerberos (criptografía simétrica). Al elaborar marcos jurídicos y normativos para reglamentar estas tecnologías, se deberá prestar atención a las de carácter múltiple. Los marcos jurídicos y normativos de los sistemas de autenticación electrónica deberán tener flexibilidad suficiente para abarcar tecnologías híbridas, porque los que se centran expresamente en tecnologías específicas pueden obstaculizar la utilización de las tecnologías múltiples[71]. La aceptación de estos criterios tecnológicos híbridos se facilitaría mediante disposiciones neutrales respecto de las tecnologías.

4. Firmas escaneadas y nombres mecanografiados

65. La razón principal del interés legislativo por el comercio electrónico en la esfera del derecho privado ha sido la inquietud respecto del efecto que las nuevas tecnologías pueden tener en la aplicación de normas de derecho concebidas para otros medios. Esta atención a la tecnología ha conducido con frecuencia, deliberadamente o no, a centrarse en tecnologías avanzadas que hacen más seguros los métodos de autenticación y firma electrónicas. En ese contexto suele perderse de vista que muchas de las comunicaciones mercantiles en el mundo, cuando no la mayoría, no utilizan ninguna tecnología concreta de autenticación o firma.

66. En la práctica cotidiana, las empresas de todo el mundo se consideran satisfechas, por ejemplo, intercambiando correos electrónicos sin ningún tipo de autenticación o firma que no sea el nombre mecanografiado, el título y la dirección de las partes al pie de sus comunicaciones. En ocasiones se les da un aspecto más oficial utilizando imágenes de firmas manuscritas reproducidas en facsímil o escaneadas, lo que, desde luego, constituye únicamente una copia digitalizada del original manuscrito. Ni los nombres mecanografiados en correos electrónicos sin cifrar ni las firmas escaneadas brindan mucha seguridad ni sirven para demostrar categóricamente la identidad del iniciador de la comunicación electrónica en que figuren. Sin embargo, las empresas deciden libremente utilizar estas formas de "autenticación" en aras de la facilidad, la conveniencia y la economía de las comunicaciones. Es importante que los legisladores y los responsables de formular las políticas tengan presentes estas prácticas mercantiles generalizadas al examinar la reglamentación de la autenticación y la firma electrónicas. Todo requisito estricto al respecto, en particular la imposición de un método o tecnología determinados, puede poner inadvertidamente en duda la validez y aplicabilidad de un número considerable de operaciones que se realizan todos los días sin utilizar ningún tipo especial de autenticación o firma. Ello, a la vez, puede incitar a las partes de mala fe a eludir las obligaciones que hayan asumido libremente impugnando la autenticidad de sus propias comunicaciones electrónicas. No es realista prever que la imposición de requisitos relativamente estrictos en materia de autenticación y firma

[71] Véase Foundation for Information Policy Research, *Signature Directive Consultation Compilation*, 28 de octubre de 1998, en que figura una recopilación de las respuestas presentadas durante las consultas sobre el proyecto de directiva de la Unión Europea acerca de la firma electrónica, preparada a petición de la Comisión Europea, disponible en www.fipr.org/publications/sigdirecon.html, (consultado el 5 de junio de 2008).

haría que todas las partes los aplicaran cotidianamente. Las experiencias recientes con métodos avanzados, como la firma digital, ha demostrado que los problemas relativos a sus costos y su complejidad limitan con frecuencia la utilidad práctica de las técnicas de autenticación y firma.

C. Gestión de la identidad electrónica

67. En el ámbito electrónico, las personas físicas o jurídicas pueden recurrir a diversos prestadores de servicios. Cuando una persona se inscribe en uno ellos para utilizar dichos servicios, se crea una "identidad" electrónica. Además, una sola identidad puede vincularse a diversas cuentas, correspondientes a cada aplicación o plataforma. La multiplicidad de identidades y cuentas puede dificultar su utilización tanto para el usuario como para el prestador de servicios. Estas dificultades podrían evitarse creando una identidad electrónica única para cada persona.

68. La inscripción ante un prestador de servicios y la creación de una identidad electrónica supone establecer una relación de confianza mutua entre la persona y el prestador. La creación de una identidad electrónica única requiere conjugar estas relaciones bilaterales en un marco más amplio que permita su gestión conjunta, en lo que se denomina gestión de la identidad. Entre las ventajas de ésta pueden figurar desde la perspectiva del prestador, mejoras de la seguridad, la facilitación del cumplimiento de las normas pertinentes y la agilización de las operaciones comerciales, así como, desde el punto de vista del usuario, la facilitación del acceso a la información.

69. La gestión de la identidad puede describirse en el contexto de los enfoques o criterios siguientes:

a) Enfoque tradicional de acceso del usuario. Este enfoque sigue el paradigma de conexión, o log-on, basado típicamente en el empleo de la información contenida, por ejemplo, en una tarjeta con memoria o en otro dispositivo en poder del cliente que éste utiliza para conectarse a un servicio. El enfoque de acceso del usuario para la gestión de la identidad se centra en la administración de la autenticación del usuario, los derechos de acceso, las restricciones a éste, los perfiles de las cuentas, las contraseñas y otras características de uno o varios sistemas o aplicaciones. El objetivo es facilitar y controlar el acceso a las aplicaciones y los recursos y proteger al mismo tiempo la información personal y comercial confidencial frente a posibles usuarios no autorizados.

b) Enfoque basado en los servicios. Este criterio representa un paradigma más innovador basado en un sistema que proporciona servicios personalizados a los usuarios y sus dispositivos. De este modo, el alcance de la gestión de la identidad se amplía y comprende todos los recursos de la empresa que se utilizan para prestar servicios en línea, como el equipo de la red, los servidores, los portales, el contenido, las aplicaciones y los productos, así como las credenciales, las libretas de direcciones, las preferencias y los derechos del usuario. En la práctica, ello puede incluir, por ejemplo, información relativa a las configuraciones de control de acceso establecidas por los padres y la participación en programas de fidelidad.

70. Se impulsan iniciativas para ampliar la gestión de la identidad en el plano empresarial y estatal. Sin embargo, cabe señalar que las opciones de política en las situaciones respectivas pueden ser muy diferentes. Concretamente, el enfoque estatal puede orientarse más a atender mejor las necesidades de los ciudadanos, y por ello estar mejor predispuesto a la interacción con personas físicas. En cambio, en las aplicaciones comerciales se debe tener presente la utilización cada vez mayor de máquinas automáticas en las operaciones comerciales, y por ello tal vez se deban adoptar elementos destinados a prever las exigencias concretas que plantean dichas máquinas.

71. Algunas de las dificultades observadas en los sistemas de gestión de la identidad son las preocupaciones relacionadas con la esfera privada derivadas de los riesgos que entraña la utilización indebida de identificadores exclusivos. Además, pueden plantearse problemas por las diferencias en las normas legales vigentes, en particular con respecto a la posibilidad de delegar la facultad de actuar en nombre de otra persona. Se han propuesto soluciones basadas en la cooperación empresarial voluntaria, dentro de lo que se llama un círculo de confianza, cuyos miembros están obligados a confiar en la corrección y exactitud de la información que les presenten otros miembros. Sin embargo, tal vez este enfoque no baste para reglamentar todas las cuestiones conexas, y requiera la adopción de un marco jurídico. Además, se han preparado directrices para establecer los requisitos legales que debería cumplir un círculo de infraestructuras de confianza[72].

72. Con respecto a la interoperabilidad técnica, la Unión Internacional de Telecomunicaciones (UIT) creó un grupo temático sobre gestión de identidades para facilitar y promover la creación de un marco genérico de gestión de identidades y de mecanismos para descubrir identidades autónomas distribuidas, así como federaciones de identidades y sus aplicaciones[73].

73. Además, se están presentando soluciones de gestión de la identidad en el contexto de la gobernación electrónica. Por ejemplo, en el marco de la iniciativa de la Unión Europea titulada "i2010: una sociedad de la información europea para el crecimiento y el empleo"[74] se puso en marcha un estudio sobre la materia para promover un enfoque coherente de la gestión de la identidad electrónica en la gobernación electrónica en el ámbito de la Unión Europea, basado en los

[72] El Liberty Alliance Project (véase www.projectliberty.org) es una alianza de más de 150 empresas, organizaciones sin fines de lucro y entidades gubernamentales de todo el mundo. Este consorcio está empeñado en establecer una norma abierta de identidad federada de red que pueda utilizarse en la red con todos los dispositivos existentes y nuevos. La identidad federada da a empresas, gobiernos, empleados y consumidores la posibilidad de controlar, en condiciones más cómodas y seguras, la información sobre la identidad en la economía digital actual y es un factor determinante para impulsar la utilización del comercio electrónico y los servicios de datos personalizados, así como los servicios basados en la web. Pueden afiliarse a ella todas las organizaciones comerciales y no comerciales.

[73] Véase http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html (consultado el 20 de marzo de 2008).

[74] Comunicación de la Comisión de las Comunidades Europeas al Consejo Europeo, el Parlamento Europeo, el Comité Económico y Social Europeo y el Comité de las Regiones: "i2010: una sociedad de la información europea para el crecimiento y el empleo", COM (2005) 229 final (Bruselas, 1º de junio de 2005, disponible en http://eur-lex.europa.eu (consultado el 20 de marzo de 2008).

conocimientos especializados existentes y en iniciativas de los Estados miembros de la Unión Europea[75].

74. Se ha hecho cada vez más habitual la distribución de dispositivos de firma electrónica, a menudo en forma de tarjetas con memoria, en el contexto de iniciativas de gobernación electrónica. Se han puesto en marcha campañas nacionales de distribución de estas tarjetas, entre otros países en Bélgica, donde se introdujeron originalmente en varias provincias en 2003[76] y, después del éxito de un periodo de prueba, se extendieron finalmente a todo el país[77]. El sistema belga supone esencialmente la emisión de tarjetas de identidad física dotadas de un pequeño circuito integrado ("chip" que contiene los datos que necesita un ciudadano para producir una firma digital[78].

75. Austria ha desarrollado un sistema de gestión de la identidad que registra las características que identifican a cada ciudadano austriaco, pero no las incorpora en los documentos oficiales de identificación de esos ciudadanos. En su lugar, establece normas de tecnología neutral que tienen por resultado el desarrollo, y la adopción por los consumidores, de numerosas soluciones tecnológicas. El sistema austriaco se basa en un "vínculo de identidad de la persona" que consiste en una estructura firmada por la autoridad pública emisora la cual asigna un rasgo único de identificación de la persona (por ejemplo, un número de registro) a uno o más certificados pertenecientes a dicha persona. De este modo, el vínculo de identidad de la persona puede utilizarse para identificarla de manera singular y automatizada cuando se dirige a la autoridad pública en el curso de un procedimiento[79]. Esta "característica singular de identificación" puede almacenarse en cualquier tarjeta con memoria que elija la persona (por ejemplo, la tarjeta de un distribuidor automático de billetes de un banco, la tarjeta de la seguridad social, la tarjeta de identificación como estudiante, la tarjeta de afiliación a un sindicato o asociación profesional, una computadora personal o una computadora portátil). Los dispositivos de firma también pueden transmitirse a través de un teléfono móvil, en forma de códigos de un solo uso, generados especialmente por el prestador de servicios de telefonía móvil que actúa de custodio de la peculiaridad singular de identificación del ciudadano.

---

[75] Véase *Modinis Study on Identity Management in eGovernment: Identity Management Issue Report* (Comisión Europea, Dirección General de Sociedad de la Información y Medios de Comunicación, 18 de septiembre de 2006), págs. 9 a 12, disponible en https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi (consultado el 6 de junio de 2008).

[76] La tarjeta de identidad electrónica fue introducida en Bélgica en 2003 en virtud de la Ley de 25 de marzo de 2003 "modifiant la loi du 8 août 1983 organisant un Registre nacional des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques" (Moniteur belge, Ed. 4, 28 de marzo de 2003, pág. 15921).

[77] Véase "Arrêté royal du 1er septembre 2004 portant la décision de procéder à l'introduction généralisée de la carte d'identité électronique" (Moniteur belge, Ed. 2, 15 de septiembre de 2004, pág. 56527). Para información general, véase http://eid.belgium.be (consultado el 6 de junio de 2008).

[78] Para información general, véase http://eid.belgium.be (consultado el 6 de junio de 2008).

[79] Zentrum für sichere Informationstechnologie Austria (A- Sit), *XML Definición del vínculo de identidad de la persona*, disponible en http://www.buergerkarte.at/koncept/personenbindung/spezifikation/aktuell/ (consultado el 6 de junio de 2008)).

76. Este sistema permite emitir identificadores específicos de un sector, que se mantienen estrictamente separados si bien todos ellos están vinculados a un almacén central de identidades. Esta arquitectura evita los problemas que supone el hecho de compartir datos, y protege su privacidad. Se pretende que la tarjeta conocida como "tarjeta del ciudadano" se convierta en el documento oficial de identidad para los procesos administrativos electrónicos, por ejemplo, la presentación de solicitudes vía Internet. La tarjeta del ciudadano establece una infraestructura de seguridad a disposición de todos, incluidos los clientes comerciales. Las empresas pueden desarrollar servicios seguros en línea para sus clientes aprovechando la infraestructura que proporciona la tarjeta del ciudadano.

77. De resultas de iniciativas como las arriba descritas, muchos ciudadanos han recibido dispositivos que, entre otras cosas, les permiten utilizar firmas electrónicas a bajo costo. Aunque el objetivo principal de estas iniciativas tal vez no sea comercial, esos mecanismos pueden utilizarse igualmente en el ámbito comercial. Cada vez se reconoce más la convergencia de los dos ámbitos de aplicación[80].

[80] Véase, por ejemplo, *2006 Korea Internet White Paper* (Seúl, Organismo Nacional de Corea para el Desarrollo de Internet, 2006) pág. 81, en que se alude a la doble utilización, en aplicaciones de gobernación electrónica y comercio electrónico, de la Ley de firmas electrónicas de la República de Corea, disponible en http://www.ecommerce.or.kr/activities/ documents_view.asp?bNo=642&Page=1 (consultado el 6 de junio de 2008).

II. Trato jurídico de la autenticación y las firmas electrónicas

78. 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 normas 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[81]; o acuerdos contractuales[82].

79. Un volumen importante de operaciones comerciales electrónicas se lleva a cabo en redes cerradas, es decir, en 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.

80. 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, existe la creciente tendencia a 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 convenidos

[81] 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 (consultado el 5 de junio de 2008).

[82] 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 (consultado el 5 de junio de 2008).

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[83]. Dentro de los límites de la libertad contractual que prevé el derecho aplicable, dichos acuerdos y reglas suelen disponer de un mecanismo de autocontrol.

81. No obstante, si no existen reglas contractuales, o en la medida en que el derecho aplicable pueda limitar su fuerza ejecutiva, 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. Enfoque tecnológico de los textos legislativos

82. La legislación y la reglamentación de la autenticación electrónica han adoptado muchas formas distintas en el plano internacional y el nacional. Cabe señalar tres enfoques principales para abordar las tecnologías de firma y autenticación, a saber: *a)* el enfoque minimalista; *b)* el enfoque específico de la tecnología; y *c)* el enfoque del doble nivel[84].

1. Enfoque minimalista

83. Algunos foros reconocen todas las tecnologías de firma electrónica, adoptando una política de neutralidad tecnológica[85]. Este enfoque o 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.

84. La Ley Modelo de la CNUDMI sobre Comercio Electrónico prevé lo que es el conjunto de criterios legislativos de uso más extendido para establecer una equivalencia

[83] 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.

[84] 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.

[85] Por ejemplo, Australia y Nueva Zelandia.

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."

85. 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.

86. 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[86].

87. Con la excepción de Europa, cuya legislación se ha visto influida principalmente por las directivas promulgadas por la Unión Europea[87], casi todos los países que han promulgado legislación relacionada con el comercio electrónico se han servido de la

---

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

[87] 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 (*Diario Oficial de las Comunidades Europeas*, L 13, 19 de enero de 2000). 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 (*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.

Ley Modelo sobre Comercio Electrónico como plantilla[88]. 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[89] y los Estados Unidos de América[90]. Con poquísimas excepciones[91], los 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

[88] A enero de 2007, se había adoptado legislación que aplicaba 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 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 de Hong Kong de 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*.

[89] 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 (consultado el 6 de junio de 2008). 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 Quebec promulgó legislación específica (Ley por la que se establece un marco jurídico para la 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.ulcc.ca, puede obtenerse información actualizada sobre la promulgación de la Ley Uniforme de Comercio Electrónico (consultado el 5 de junio de 2008).

[90] En los Estados Unidos, 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 6 de junio de 2008). 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, Hawai, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, 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 (consultado el 6 de junio de 2008).

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

Modelo de la CNUDMI sobre Firmas Electrónicas, que fue aprobada en 2001, como la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, más reciente (que fue aprobada por la Asamblea General por su resolución 60/21, 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*, párr. 95).

88. Cuando la legislación adopta el enfoque 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.

89. 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 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 o 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. Enfoque de la tecnología específica

90. 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 por conseguir

el máximo nivel de seguridad que ofrece la tecnología existente[92]. 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, 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 en actas notariales). En el marco de un enfoque de tecnología específica, la normativa impondría una tecnología específica que cumpliera los requisitos legales para dar validez a 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 enfoque o criterio "prescriptivo".

91. El enfoque 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"[93]. 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 sobre la tecnología específica corre el riesgo de establecer requisitos antes de que una tecnología concreta se consolide[94]. 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 al 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 podrían ocasionar

[92] Uno de los primeros ejemplos fue la Ley de firma digital de Utah, aprobada en 1995 pero derogada a partir del 1º de mayo de 2006 por la Ley estatal 20, disponible en http://www.le.state.ut.us/~2006/htmdoc/sbillhtm/sb0020.htm (consultado el 6 de junio de 2008). 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).

[93] 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 6 de junio de 2008).

[94] No obstante, teniendo en cuenta que la ICP está ya bastante consolidada y establecida, puede que algunas de estas preocupaciones no tengan actualmente el mismo peso.

gastos y esfuerzos excesivos, lo que tal vez obstaculizaría la difusión del comercio electrónico.

92. La legislación sobre 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 varios, 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)[95];

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 interactuar con la alta autoridad para que sus símbolos de autenticación (u otros medios destinados al mismo fin) sean aceptados fuera de sus propios sistemas. En este caso, 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[96];

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[97]. Los sistemas de gestión de la identidad (véanse los párrs. 67 a 77 *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.

[95] 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, donde se cita a los Estados Unidos como ejemplo de la aplicación de este modelo.

[96] Véase Foro de Cooperación de Asia y el Pacífico, *Assessment Report*…, donde se cita como ejemplo a Singapur.

[97] Véase Foro de Cooperación de Asia y el Pacífico, *Assessment Report*…, donde se cita como ejemplos a China y Malasia.

3. Enfoque del doble nivel

93. Según este enfoque, la legislación establece un umbral bajo de requisitos para que los métodos de autenticación electrónica reciban una determinada condición jurídica mínima 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)[98]. 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 ICP.

94. Suele optarse por este enfoque 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 enfoque 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. Estos 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 enfoque del 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 enfoque de la tecnología específica (véase *supra*, párrs. 90 a 92). 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 ordenamientos jurídicos reconocerían únicamente a los prestadores de servicios de certificación autorizados como posibles emisores de certificados “seguros” o “reconocidos”.

[98] Aalberts y van der Hof, *Digital Signature Blindness ...* , párr. 3.2.2.

95. Entre los primeros foros que han aprobado legislación por la que se adopta el enfoque del doble nivel figuran Singapur[99] y la Unión Europea[100]. Les siguieron otros ordenamientos jurídicos[101]. La Ley Modelo de la CNUDMI sobre Firmas Electrónicas autoriza al Estado promulgador a establecer un sistema de doble nivel mediante la reglamentación pertinente, aunque no lo promueve activamente[102].

96. 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.)[103]. Además, se sugirió que la legislación sobre el doble nivel diera 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.

---

[99] 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.

[100] Al igual que la Ley de operaciones electrónicas de Singapur, la Directiva de la Unión Europea sobre la firma electrónica (*Diario Oficial de las Comunidades Europeas*, L 13/12, 19 de enero de 2000), 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 "*a)* 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.).

[101] Por ejemplo, Mauricio y el Pakistán. Véanse detalles de las respectivas normas legislativas en la nota 88 *supra*.

[102] La Ley Modelo de la CNUDMI sobre Firmas Electrónicas, 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.

[103] Baker y Yeo, "Background and issues concerning authentication ...".

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

97. 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 los basados 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 atribución general de los registros electrónicos

98. En la utilización de métodos de autenticación electrónicos hay dos aspectos de interés para el presente examen. El primero es la cuestión general de la atribución 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.

99. 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[104], 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 "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 de un mensaje de datos ni establecer la identidad de las partes. Se refiere más bien a la atribución de los mensajes, estableciendo las condiciones en que una parte puede dar por sentado que un determinado mensaje de datos provenía efectivamente del supuesto iniciador.

[104] Publicación de las Naciones Unidas, núm. de venta: S.99.V.11, disponible en http://www.uncitral.org/pdf/spanish/texts/payments/transfers/ml-credittranss.pdf (consultado el 6 de junio de 2008).

100. 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 lo ha enviado efectivamente. 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 proviene del iniciador: en primer lugar, aquéllas en que el destinatario haya aplicado adecuadamente un procedimiento de autenticación aceptado previamente por el iniciador; y, en segundo lugar, 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.

101. 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[105]. Algunos países se refieren expresamente a la utilización de códigos, contraseñas u otros medios de identificación como factores que crean la presunción de autoría[106]. 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 atribución[107].

102. 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[108]. Además, varios países que han aplicado la Ley Modelo sobre Comercio Electrónico no han incorporado disposiciones concretas basadas en su artículo 13[109]. 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 atribuir el mensaje, como en el caso 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 varía en el caso de las firmas electrónicas"[110].

---

[105] 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 Jersey, dependencia de la Corona Británica (art. 8), y en los Territorios británicos de ultramar de las Bermudas (art. 16, párr. 2) y Turcos y Caicos (art. 14). Los pormenores de las leyes respectivas figuran en la nota 88 *supra*.

[106] México (véase la nota 88 *supra*), art. 90, párr. I.

[107] Por ejemplo, la Ley Uniforme de operaciones electrónicas de los Estados Unidos (véase la nota 90) dispone, en el apartado *a)* del artículo 9, que un registro o 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 apartado *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 apartado *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."

[108] Australia (art. 15, párr. 1); en lo esencial del mismo modo, Eslovenia (art. 5); India (art. 11); y Pakistán (art.13, párrafo 2). Véase también Isla de Man, dependencia de la Corona Británica (art. 2);y Región Administrativa Especial de Hong Kong de China (art. 18). Los pormenores de las leyes respectivas figuran en la nota 88 *supra*.

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

[110] Canadá, Ley Uniforme de comercio electrónico (con comentario oficial) (véase la nota 89), comentario del artículo 10.

103. Sin embargo, otros países han preferido separar las disposiciones de la Ley Modelo sobre Comercio Electrónico relativas a la atribución de las relativas a la firma electrónica. Ello se basa en el entendimiento de que la atribución 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"[111]. Esta norma general sobre atribución 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"[112]. 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 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

[111] Estados Unidos, Ley Uniforme de operaciones electrónicas (1999) (véase la nota 90), 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".

[112] 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 transmisión 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.".

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 asigne a dicho procedimiento de seguridad como elemento para determinar la autoría[113]."

104 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"[114].

105. 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[115]. 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[116]. 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 justificar un dictamen de autoautenticación"[117]. Los tribunales tienden a tener en cuenta todas las pruebas existentes y no rechazan la documentación electrónica por razón de presunta inadmisibilidad.

106. 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[118]. Otros ejemplos de un enfoque más restrictivo del valor probatorio de los documentos

---

[113] Comentario oficial sobre el artículo 9.

[114] Párrafo 6 de los comentarios oficiales sobre el artículo 9.

[115] *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. 235, pág. 916.

[116] *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.

[117] *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.

[118] 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, disponible en http://www.jurpc.de/rechtspr/20020332.htm (consultado el 6 de junio de 2008).

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[119], 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[120]. El oferente de bienes o 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 los mensajes enviados por un sitio de Internet con la contraseña de acceso de dicha persona a ese sitio[121]. 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[122].

2. Posibilidad de cumplir los requisitos de firma

107. En algunos países, los tribunales han tendido a interpretar con flexibilidad los requisitos de firma. Como se indicó antes (véase la introducción, párrs. 2 a 4), 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

[119] 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, disponible en http://www.jurpc.de/rechtspr/20020071.htm (consultado el 6 de junio de 2008); 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, disponible en http://www.jurpc.de/rechtspr/20040074.htm (consultado el 6 de junio de 2008).

[120] Alemania, Landesgericht (Tribunal del Land) , 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, disponible en http://www.jurpc.de/rechtspr/20020291.htm (consultado el 6 de junio de 2008).

[121] 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, disponible en http://www.jurpc.de/rechtspr/20020136.htm (consultado el 6 de junio de 2008).

[122] Alemania, Oberlandesgericht Köln (Tribunal de apelación), 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, disponible en http://www.jurpc.de/rechtspr/20020364.htm (consultado el 6 de junio de 2008).

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[123]. Y 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[124]. Se considera autenticación válida el acto deliberado de una persona de mecanografiar su nombre al pie de todos sus mensajes por correo electrónico[125]. 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[126] 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 en un documento o su membrete bastan para cumplir el requisito de firma"[127]. Si las partes no niegan haber 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"[128].

108. 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"[129]. 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

[123] *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.

[124] *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.

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

[126] *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.

[127] Ibíd., pág. 919: "Pueden utilizarse documentos internos, facturas y correos electrónicos para cumplir la legislación sobre el fraude de Illinois [Código de Comercio Uniforme]". Sin embargo, en este caso concreto, el tribunal dictaminó que el supuesto contrato no cumplía la Ley contra el fraude, no porque los mensajes de correo electrónico no sirvieran como tales para consignar válidamente las condiciones de un contrato, sino porque no había indicios de que los autores de los correos electrónicos y las personas mencionadas en ellos fueran empleados del demandado.

[128] *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.

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

electrónicamente y no en formato impreso no significa nada"[130]. En ocasiones, los tribunales han rechazado los argumentos en el sentido de que el correo electrónico constituya un contrato firmado a efectos de la Ley contra el 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 contra el 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 negociación"[131]. 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"[132]. Aunque los tribunales británicos parecen interpretar los requisitos de forma previstos en la Ley contra el 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 legislación determinada, siempre que el método en cuestión cumpla la misma función que la firma manuscrita[133].

109. 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[134]. Se observa una postura ligeramente más flexible en algunos fallos en que se acepta la presentación electrónica de recursos

---

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

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

[132] *Mehta contra J. Pereira Fernandes S.A…*

[133] *Mehta contra J. Pereira Fernandes S.A*…, 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 este 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]".

[134] 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 contra M. X.*, disponible en www.juriscom.net/jpt/visu.php?ID=239) (consultado el 6 de junio de 2008).

administrativos para cumplir un plazo legal, al menos si se confirman posteriormente por correo ordinario[135].

110. A diferencia del criterio restrictivo aplicado a la atribución 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[136] y el Tribunal Federal de Justicia[137] 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, 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[138]. Esta 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[139].

111. 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[140], 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,

---

[135] Francia, Consejo de Estado, 28 de diciembre de 2001, N° 235784, *Élections municipales d'Entre-Deux-Monts* (original disponible en la Secretaría).

[136] 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, disponible en www.jurpc.de/rechtspr/19980009.htm (consultado el 6 de junio de 2008).

[137] 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, disponible en http://www.jurpc.de/rechtspr/19990005.htm (consultado el 6 de junio de 2008).

[138] Ibíd.

[139] En un fallo relativo a una causa que le remitió el Tribunal Federal de Justicia de Alemania, la Sala Conjunta de los Tribunales Federales Superiores 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 telex o el fax. Sostuvo además 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- für Zeitschrift Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. Nº 160/2000, disponible en http://www.jurpc.de/rechtspr/20000160.htm (consultado el 6 de junio de 2008).

[140] 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).

porque en las comunicaciones se utilizaban métodos que permitían identificar a las partes[141].

112. 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. 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. Labor encaminada a crear equivalentes electrónicos de formas especiales de firma

a) Aplicaciones internacionales: apostillas electrónicas

113. Del 28 de octubre al 4 de noviembre de 2003 se reunió en La Haya una comisión especial para examinar el funcionamiento práctico del Convenio sobre la Eliminación del Requisito de la Legalización de Documentos Públicos Extranjeros (Convenio de La Haya sobre Apostillas), el Convenio sobre la Notificación o Traslado en el Extranjero de Documentos Judiciales o Extrajudiciales en Materia Civil o Comercial[142] (Convenio de La Haya sobre Notificación) y el Convenio sobre la obtención de pruebas en el extranjero en materia civil o mercantil (Convenio de La Haya sobre Obtención de Pruebas)[143]. A la reunión de la Comisión Especial sobre el funcionamiento práctico de los Convenios de La Haya sobre Apostillas, Notificación y Obtención de Pruebas asistieron 116 delegados en representación de 57 Estados Miembros, Estados parte en uno o más de los convenios examinados así como observadores. La Comisión Especial destacó que los tres Convenios funcionaban en un entorno sometido a importantes

[141] 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 (disponible en http://www.camara-e.net/_upload/80403--0-7-diaz082003.pdf) (consultado el 6 de junio de 2008).

[142] Naciones Unidas, *Treaty Series*, vol.658, Nº 9432.

[143] Ibíd., vol. 847 Nº 12140.

progresos técnicos. Aunque esta evolución no pudo preverse en el momento de aprobar los tres Convenios, la Comisión Especial destacó que las tecnologías modernas formaban parte integrante de la sociedad actual y que su utilización constituía un hecho incontrovertible[144]. La Comisión Especial observó a este respecto que el espíritu y la letra de los Convenios no constituían un obstáculo para el empleo de tecnologías modernas y que su aplicación y funcionamiento podía mejorarse aún más basándose en tales tecnologías[145]. La Comisión Especial recomendó que los Estados partes en los Convenios, y la Mesa Permanente de la Conferencia de La Haya de Derecho Internacional Privado, contribuyeran al desarrollo de técnicas para la obtención de apostillas electrónicas "teniendo en cuenta entre otras cosas las leyes modelo de la CNUDMI sobre comercio electrónico y sobre firmas electrónicas, basadas ambas en los principios de no discriminación y equivalencia funcional"[146]. 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 dicho programa, 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)[147]. El programa prevé dos formatos distintos, pero en definitiva idénticos, para las apostillas-e. Ambos métodos protegen el documento inicial y el certificado de la apostilla-e frente a modificaciones no autorizadas, pero cada uno presenta al receptor una interfaz diferente.

114. Con arreglo al primer método, la autoridad competente puede añadir el certificado de la apostilla como última página de un documento público inicial ya existente, en un formato determinado. El e-APP prevé que los documentos se intercambien en el formato portátil de documentos (PDF). El receptor abrirá el archivo y encontrará el certificado de apostilla-e incluido como última página del documento. Si se elije este formato, el documento público original y el certificado de apostilla-e forman un documento continuo o, dicho de otro modo, un solo archivo electrónico. También cabe escoger la impresión de una o varias páginas de este archivo único, de forma que el certificado de apostilla-e pueda imprimirse por sí mismo[148].

115. Con arreglo al segundo método, el documento público original se adjunta como archivo aparte al certificado de apostilla-e. El receptor sigue recibiendo un solo archivo PDF pero, al abrirlo, el usuario ve en primer lugar el certificado de apostilla

[144] 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, Notificación y Obtención de Pruebas: 28 de octubre a 4 de noviembre de 2003", párr. 4, disponible en http://hcch.e-vision.nl/upload/wop/lse_concl_e.pdf (consultado el 6 de junio de 2008).

[145] Conferencia de La Haya de Derecho Internacional Privado, "Conclusiones y recomendaciones adoptadas por la Comisión Especial …".

[146] Conferencia de La Haya de Derecho Internacional Privado, "Conclusiones y recomendaciones adoptadas por la Comisión Especial…", párr. 24.

[147] Christophe Bernasconi y Rich Hansberger, "Programa experimental de apostillas electrónicas (e-APP): memorando sobre algunos aspectos técnicos en que se basa el método sugerido para emitir apostillas electrónicas (apostillas-e)", disponible en http://www.hcch.net/upload/wop/genaff_pd18e2007.pdf (consultado el 26 de mayo de 2008).

[148] "Programa experimental de apostillas electrónicas...", párr. 18.

electrónica y a continuación puede abrir el documento público original adjunto para verlo como archivo PDF independiente. Se ha dicho que este método proporciona una interfaz más intuitiva al receptor del documento objeto de la apostilla (por ejemplo, lo ha adoptado el Departamento del Estado de los Estados Unidos para sus archivos electrónicos de patentes y como modelo de las apostillas electrónicas). El hecho de adjuntar el documento público de que se trata a un archivo del certificado de apostilla electrónica constituye un intento de que quede muy claro para el receptor cuando abra por primera vez el documento que se trata de una apostilla. A partir de entonces, el receptor puede abrir el documento público de que se trata para ver su contenido"[149].

116. En ambos modelos, el funcionamiento práctico de las apostillas electrónicas supone la emisión de certificados en forma electrónica firmados digitalmente por la autoridad competente a la que le corresponda a efectos del Convenio de La Haya sobre Apostillas. Cada autoridad competente mantendría además un registro en forma electrónica que permitiera verificar los certificados emitidos en apoyo de las apostillas electrónicas[150].

117. En los países que han suprimido los requisitos de legalización o de apostilla, cabe concebir la posibilidad de desarrollar sistemas en virtud de los cuales las actas notariales extranjeras puedan ser reconocidas jurídicamente basándose en la verificación del método de firma o autenticación electrónico utilizado por el notario que origina estas actas. El usuario del documento (en general otro notario) tiene que poder verificar la firma electrónica del primer notario de manera sencilla y rápida. Esto puede hacerse por Internet accediendo al sitio del prestador de servicios que origina la certificación del notario inicial que, por lo menos en Europa, suele ser la cámara o colegio nacional a que pertenece el notario. Una manera parecida consiste en verificar la autoridad del notario inicial para autenticar actas en el ordenamiento jurídico en que actúa. Para facilitar este proceso y que no sea necesario consultar a un órgano supervisor extranjero, caso de haberlo, encargado de facultar el ejercicio de la profesión notarial, se ha propuesto que los prestadores de servicios de certificación establecidos bajo los auspicios de los colegios de notarios sólo expidan certificados a los notarios autorizados en el momento presente a ejercer las funciones de notario público, de manera que toda suspensión o revocación de la autoridad notarial impida automáticamente verificar la firma del notario[151].

b) Aplicaciones nacionales: Sellos, certificación notarial y atestiguación

118. 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)[152].

---

[149] "Programa Experimental de Apostillas Electrónicas…", párr. 19.

[150] Véase más información sobre el funcionamiento de las apostillas electrónicas en el sitio web de e-APP, en http://www.e-app.info/ (consultado el 6 de junio de 2008).

[151] Ugo Bechini y Bernard Reynis, "La signature électronique transfrontalière des notaires: une réalité européenne" *La semaine juridique (édition notariale et immobilière)*, Nº 39, 24 de septiembre de 2004, pág. 1447.

[152] 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 43, 1987).

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[153]. En el Canadá se prevé que los requisitos de 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[154].

119. 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 de propiedad. 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 vía 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[155].

120. La Ley Uniforme sobre el registro electrónico de bienes raíces de los Estados Unidos[156] 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 en toda ley, reglamento o norma en que se exija la presencia de un timbre, impresión o sello personal o empresarial bastará una firma electrónica. Esos indicios físicos no se pueden aplicar en 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[157]. De este modo, el timbre o impresión notarial exigidos con arreglo a las leyes de algunos Estados no se requieren en el caso de una certificación notarial

---

[153] Irlanda, Ley de comercio electrónico, artículo 16. Sin embargo, en caso de que el documento sellado deba o pueda 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.

[154] 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 Federal sobre Bienes Inmuebles.

[155] Ejemplos de ello son los requisitos relativos a la validación de documentos por profesionales autorizados o registrados, por ejemplo, en la Ley sobre los profesionales de ingeniería y geociencias (Manitoba (Canadá), en la que se define el "sello electrónico" como la forma de identificación expedida por la Asociación de Profesionales de Ingeniería y Geociencias de la provincia de Manitoba a cualquier miembro de la Asociación, 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 6 de junio de 2008).

[156] La Ley uniforme del registro electrónico de operaciones inmobiliarias de los Estados Unidos fue elaborada por la Conferencia Nacional de Comisarios de Leyes Uniformes de los Estados y está disponible en http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm (consultado el 6 de junio de 2008). Se ha adoptado en Arizona, Arkansas, Carolina del Norte, Carolina del Sur, Connecticut, Delaware, Distrito de Columbia, Florida, Idaho, Illinois, Kansas, Minnesota, Nevada, Nuevo México, Tennessee, Texas, Virginia, Washington y Wisconsin (véase http://www.nccusl.org (consultado el 20 de marzo de 2008).

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

electrónica en virtud de esta ley. Tampoco es necesario que se verifique la actuación del directivo de una empresa mediante un timbre o impresión correspondiente a ella, como se requeriría en otros casos conforme a la legislación de algunos estados.

121. Los sellos no suelen utilizarse frecuentemente en los documentos privados de los foros de derecho civil, aunque en su mayor parte estos foros emplean ampliamente las certificaciones notariales como medio de garantizar la identidad de las personas y la autenticidad de los documentos. En varios foros de derecho civil los notarios ya han introducido tecnologías de la información y las telecomunicaciones como instrumento habitual de su labor. En muchos países, los colegios de notarios han establecido prestadores de servicios de certificación para emitir certificados en apoyo de la utilización de las firmas electrónicas (generalmente firmas digitales) por los notarios afiliados a esos colegios, y a veces también por el público en general.

122. En Italia, el 12 de septiembre de 2002 la Autoridad de Tecnología de la Información en el Gobierno autorizó al Consejo del Notariado a ofrecer servicios de certificación a los notarios italianos, cuyas firmas digitales pueden verificarse en línea[158]. Además, los notarios italianos están a punto de completar el proceso de utilización de tecnologías electrónicas para la transmisión de actas a los registros públicos. Por ejemplo, los documentos en papel ya se han eliminado completamente en la transmisión de memorandos y artículos de asociación y sus modificaciones a los registros comerciales. También se han registrado progresos notables en lo que respecta a la transmisión electrónica de actas de transacciones relativas a la propiedad inmobiliaria, si bien todavía se utilizan los documentos en papel supuestamente por los retrasos que registra la introducción de las tecnologías de comunicación electrónica en los tribunales. Estos servicios se prestan mediante el apoyo de una empresa establecida especialmente en 1997 por el Consejo y el Fondo Nacional del Notariado para ocuparse de los servicios de las tecnologías de la información y la comunicación destinados a los notarios italianos[159]. En España se utiliza un sistema similar en el que el Consejo del Notariado estableció su propia autoridad certificadora y los notarios han elaborado un sistema de archivo electrónico de actas en los registros mercantiles[160].

123. En Francia, el texto revisado del artículo 1317 del Código Civil, permite, por ejemplo, registrar los "actos auténticos" utilizando medios electrónicos en las condiciones que establezca el Consejo de Estado. El Alto Consejo del Notariado de Francia ha establecido un sistema de certificación de las firmas digitales que utilizan las notarías del país[161]. El sistema empleado por las notarías francesas lo certifica una corporación establecida por varios organismos del Gobierno para ofrecer servicios de certificación. Aunque las notarias francesas todavía no utilizan la transmisión electrónica de actas en el mismo grado que las de Italia y España, el desarrollo en mayo de 2006 de la aplicación de Télé@actes debería permitir que las notarías intercambiasen los registros hipotecarios de las escrituras de propiedad de forma totalmente electrónica.

[158] Véase http://ca.notariato.it (consultado el 6 de junio de 2008).

[159] Véase www.notariato.it , en "Servizi Notartel" (consultado el 6 de junio de 2008).

[160] Véase http://www.notariado.org/n_tecno (consultado el 6 de junio de 2008).

[161] "La signature électronique notariale certifiée", *La revue fiscale notariale*, Nº 10, octubre de 2007, Alerte 53.

También está en curso la labor de digitalizar los documentos en papel de las escrituras de bienes inmuebles.

124. En Alemania, la Ley Federal de 1993 para agilizar los procedimientos de registro[162] hizo posible efectuar en forma electrónica los trámites legales de inscripción de las transacciones inmobiliarias, comerciales y de otra índole. Las administraciones judiciales subnacionales han aprovechado esta posibilidad en mayor o menor grado y mediante diversos enfoques técnicos[163]. La introducción de un sistema de registros electrónicos permitió que los notarios alemanes intercambiaran directamente información con los registros mediante comunicaciones electrónicas. Para garantizar que las actas notariales electrónicas ofrezcan el mismo nivel de confianza que las escrituradas en papel, las notarías alemanas establecieron un prestador de servicios de certificación de conformidad con los requisitos de la Ley de Firmas Electrónicas del país. El 15 de diciembre de 2000, el regulador de telecomunicaciones alemán concedió una licencia al prestador de servicios de certificación. Como ya había ocurrido en otros países, el sistema de certificación establecido por los notarios alemanes se basa en la ICP mediante la utilización de la tecnología de la firma digital. Los certificados emitidos por el prestador de servicios de certificación de la Cámara Federal de Notarios no solo certifican la clave pública utilizada por el notario para firmar documentos sino también la autoridad del firmante en su calidad de fedatario público. En el ordenamiento jurídico alemán las firmas digitales se utilizan para autenticar las actas, tanto en el momento en que se producen como cuando se reproducen. En las directrices publicadas por la Cámara Federal de Notarios, se recuerda a estos la necesidad de garantizar la transmisión segura de los documentos electrónicos, por ejemplo, utilizando únicamente conexiones SSL-seguras[164]. Para facilitar el procesamiento de las actas electrónicas por los registros o su utilización por los clientes, los notarios alemanes tienen que crear documentos en un formato estándar (Extensible Markup Language, o XML)[165].Las normas alemanas para emitir actas electrónicas auténticas requieren una doble autenticación por parte del notario. Todas las actas electrónicas, junto con sus anexos y los archivos que contienen la firma digital del notario, están vinculadas y archivadas conjuntamente en el formato de archivo ZIP, y todo ese archivo ZIP vuelve a autenticarse con la firma digital del notario.

125. Los equivalentes electrónicos de las actas notariales también se utilizan cada vez más en Austria. Las características básicas del ordenamiento jurídico austriaco para la certificación notarial electrónica son en general similares a las del sistema alemán. No obstante el ordenamiento austriaco tiene la característica particular de

---

[162] Germany Bundesgesetzblatt, primera parte, 20 de diciembre de 1993, pág. 2182.

[163] Véase la información acerca del alcance de la aplicación de registros electrónicos en Alemania por el Colegio Federal de Notarios, en http://www.bnotk.de/Service/Elektronischer_Rechtsverkehr/Registerelektronisierung.html (consultado el 6 de junio de 2008).

[164] Véase "*Empfehlungen zur sicheren Nutzung des Internet*", Rundscheiben 13/2004 der Bundesnotarkammer vom 12.03.2004, disponible en http://www.bnotk.de/Service/Rundschreiben/RS.2004.13.sichere.Interneinutzung.html (consultado el 6 de junio de 2008).

[165] Véase "*Hinweise und Anwendungsempfehlungen für den elektronischen Handels-Genossenschafts- und Partnerschaftsregisterverkehr*", Rundschreiben 25/2006 der Bundesnotarkammer vom 07.12.2006, disponible en http://www.bnotk.de/Service/Empfehlungen+Hinweise/RS25-06_El-Handelsregisterverkehr.html) (consultado el 6 de junio de 2008).

contar con un registro electrónico centralizado ("cyberDOC") para la conservación segura de los documentos en forma electrónica. Una empresa independiente establecida conjuntamente por la Cámara del Notariado Austriaca y Siemens AG proporciona a los notarios un archivo electrónico que comprende funciones de autenticación[166]. Los notarios están obligados por ley a registrar y almacenar en este archivo todas las escrituras notariales validadas después del 1º de enero de 2000.

126. Aunque por lo general la función de autenticación del notario respecto de las firmas puede reproducirse en un entorno electrónico utilizando los correspondientes métodos de autenticación y firma, otras funciones requieren soluciones más amplias. En general las actas notariales tienen que mencionar, según proceda, la fecha en que se formalizan, la fecha en que se registran y la fecha en que se firman o copian. Se ha sugerido que la simple utilización de técnicas automáticas puede sustituir la certificación de la fecha por el notario[167].

127. Mayor importancia tienen no obstante los procedimientos para mantener los registros electrónicos de las actas notariales. En general, la ley obliga a los notarios a mantener un registro de los documentos que reciben o producen. La reproducción del registro general en un entorno electrónico plantea diversos problemas. Uno de ellos -muy importante- se refiere al riesgo de incompatibilidad técnica entre los diferentes programas y equipos informáticos que pueden utilizar los notarios para el indicado fin. La rápida evolución de las tecnologías de la información y las comunicaciones aumenta la necesidad de pasar datos de un formato o medio a otro. Sin embargo, no siempre está garantizada la posibilidad de leer los datos trasladados a nuevos formatos y medios, lo que hace necesario idear procedimientos de control que permitan verificar la integridad de los contenidos de un registro antes y después de su traslado. Como ya se ha señalado anteriormente, la tecnología criptográfica basada en la ICP no siempre garantiza la posibilidad de lectura de las propias firmas digitales con el transcurso del tiempo (véase el párrafo 51 *supra*.) Ello requiere una gestión cuidadosa del proceso de traslado, y quizá la confirmación de la autenticación utilizada originalmente. Se ha llegado a la conclusión de que para garantizar la coherencia y la interoperabilidad, es preferible encargar esta función a un tercero de confianza, en vez de confiarla a cada notario[168].

128. Este fue, por ejemplo, el modelo escogido finalmente por los legisladores en Francia. La reforma reciente de las normas que rigen los registros notariales establecieron en general las condiciones necesarias para la equivalencia funcional entre las actas notariales en papel y los registros electrónicos[169]. En las disposiciones relativas principalmente a la seguridad de la información, las nuevas normas establecieron un archivo centralizado de las actas notariales en forma electrónica

[166] Véase Österreichische Notariatskammer (Cámara del Notariado Austriaca), disponible en http://www.notar.at, en el sitio "Cyberdoc" (consultado el 6 de junio 2008).

[167] Didier Froger, "Les contraintes du formalisme et de l'archivage de l'acte notarié établi sur support dématérialisé", *La semaine juridique (édition notariale et immobilière)* Nº 11, 12 de marzo de 2004, pág. 1130

[168] Didier Froger, "Les contraintes du formalisme…".

[169] Francia, "Décret nº 2005-973 du 10 août 2005 modifiant le décret nº 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires". Journal Officiel, 11 de agosto de 2005, pág. 96.

que garantice que los registros de esta clase se mantengan de tal manera que se conserve su integridad, sólo sean accesibles a los notarios que los originaron, sean trasladados a nuevos formatos ajustándose a las necesidades técnicas sin alterar su contenido y puedan registrar información posterior del notario sin alterar su contenido original.

129. A pesar de los progresos registrados en los últimos años, persisten algunas dudas acerca de cómo las nuevas normas que autorizan la equivalencia electrónica de las actas notariales en papel pueden conciliarse con los elementos esenciales de las actas auténticas, en particular, la necesidad de la presencia física de las partes ante el notario[170]. En el supuesto de que la presencia física sea indispensable para establecer un acta jurídica autentica, el problema es elaborar posibles adaptaciones de formas ya existentes a tecnologías futuras[171]. Se ha dicho a este respecto que la criptografía no sustituye los símbolos tangibles de la autoridad pública ni el consentimiento de las partes[172]. Por ello, algunas normas requieren que las partes y los testigos puedan ver realmente una imagen de su firma en la pantalla. De manera similar, en todas las actas tiene que aparecer una imagen del sello del notario[173].

130. En los Estados Unidos hay tres leyes principales sobre la certificación notarial: la Ley Uniforme de Transacciones Electrónicas[174], la Ley de Firma Electrónica en el Comercio Mundial y Nacional (firma-e)[175] y la Ley Uniforme de Registro de Operaciones Inmobiliarias[176]. 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 uno u otra. Varios estados han elaborado posteriormente sistemas de certificación notarial por medios electrónicos. Por ejemplo, el Departamento de Estado de Pennsylvania, junto con un equipo especial de registradores de condado, han elaborado el Programa de Registro y Sello Notarial Electrónico que permite a los notarios proceder a la autenticación en tiempo real y entregar en línea los sellos notariales electrónicos verificados. Este sistema de certificación notarial electrónica tiene por finalidad agilizar las transacciones comerciales entre funcionarios públicos y empresas y aumentar la protección del público frente a falsificaciones y fraudes, manteniendo al mismo tiempo los componentes fundamentales de la certificación notarial. El sistema utiliza servicios de certificación digital de un prestador de servicios comercial[177].

---

[170] Pierre-Yves Gautier y Xavier Linant de Bellefonds, "De l'écrit électronique et des signatures qui s'y attachent", *La semaine juridique (édition générale)*, nº 24, 14 de junio de 2000, I 236, sects. 8-10.

[171] Pierre Catala, "Le formalisme et les nouvelles technologies", *Répertoire du notariat Defrénois*, Nº 20, 2000, págs. 897 a 910.

[172] Luc Grynbaum, "Un acte authentique électronique pour les notaires ", Communication Commerse électronique, nº 10, octubre de 2005, com. 156.

[173] Decreto Nº 71-941, modificado por el decreto Nº 2005-973, art. 17, párr. 3 (véase la nota 169).

[174] Véase la nota 90.

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

[176] Véase la nota 156.

[177] Anthony Garritano, "National e-notary standards in progress", *Mortgage Servicing News* (Nueva York), vol. 10, Nº 2, 1º de marzo de 2006, pág. 11.

131. Los notarios interesados en participar en esta iniciativa de certificación electrónica tienen que solicitar a la Oficina de Comisiones, Elecciones y Legislación del estado su designación como notario electrónico aprobado (notario-e). El fedatario público tiene que obtener, mediante el pago de unos derechos, un certificado digital en forma de sello notarial electrónico que facilita la autoridad de certificación facultada a nivel federal, aprobada por la Oficina de Administración y del Secretario de la Commonwealth de Pennsylvania y seleccionada por los registradores de títulos legales que participen en la iniciativa. Antes de obtener el certificado digital, el notario-e reconocido tiene que comparecer personalmente ante uno de dichos registradores y presentarle la carta de reconocimiento del Departamento de Estado y pruebas satisfactorias de su identidad. En lo que respecta a cada certificación electrónica, el notario-e reconocido tiene que garantizar que se adjunte, o esté asociada lógicamente, a la firma o el acta electrónica que se protocoliza, reconoce o verifica la información siguiente: nombre completo del notario-e, acompañado de las palabras "notario público", nombre del municipio y condado en que el notario tiene una oficina y fecha en que expirará el mandato del notario. Éste tiene que asegurarse de que la persona para la que efectúa una certificación electrónica comparezca personalmente ante él en cada una de estos actos. Con arreglo a lo establecido por el Departamento de Estado de Pennsylvania, seguirán aplicándose los componentes fundamentales de la certificación, incluida la comparecencia personal de los firmantes de documentos ante el notario. No obstante, en sustitución del documento en papel y la estampación del sello notarial con un sello de goma, el notario agrega digitalmente su información identificadora a un documento que existe como datos electrónicos en forma legible por computadora[178].

132. De manera muy parecida a lo que ocurre en los foros romanistas, en los de derecho anglosajón se ha debatido la capacidad de los medios electrónicos para reproducir la función de los métodos tradicionales de certificación y autenticación. En tanto en cuanto la certificación se limite esencialmente a confirmar la integridad de documentos y la identidad de los firmantes, no parece que existan dificultades insuperables para utilizar las comunicaciones electrónicas en sustitución de los documentos en papel. En cambio, la situación está menos clara cuando la autenticidad de un documento o un acta se certifica mediante la confirmación por el notario de la presencia de la persona en el momento en que se formaliza el documento o el acta[179].

---

[178] Véase http://www.dos.state.pa.us/dos/site/default.asp, en "Notaries", "Electronic Notarization" (consultado el 5 de junio de 2008).

[179] "La tecnología actual que permite las 'teleconferencias' entre las partes en diferentes ciudades, o incluso diferentes naciones, hará que en el futuro probablemente existan definiciones legales más amplias de la 'comparecencia personal', por la que un notario de Los Ángeles pueda legalizar la firma vista por televisión de una persona que se encuentre en Londres. La interacción acústica del notario con el firmante ausente y la obtención en tiempo real de la imagen de video del firmante parecen ser requisitos previos indispensables para realizar esas certificaciones electrónicas remotas. Sin embargo, si bien estas actas notariales electrónicas, en la que el notario se encuentra en un lugar y el certificador o declarante en otro, son por lo menos concebibles sin una interacción auditiva, tal como demuestra la extensa utilización del correo electrónico, la interacción visual parece una condición ineludible. Cómo si no podría determinar el notario que un firmante remoto no es objeto de una coacción flagrante y registrar una imagen visual que proporcione la prueba de que el transmisor no es un impostor que utiliza una clave privada robada. Al igual que en 1984 la Corte Suprema de Nebraska (*Christensen contra Arant*) falló que el simple contacto auditivo a través de una puerta no era suficiente para demostrar la presencia física en el sentido jurídico tradicional, también es probable que el simple contacto electrónico a través de un medio no visual no sea suficiente para demostrar la presencia física en el sentido jurídico futuro" (Charles N. Faerber, "Being there: the importance of physical presence to the notary ", *The John Marshall Law Review*, vol. 31, primavera de 1998, págs. 749 a 776).

133. Se ha afirmado que los procedimientos tradicionales de atestiguación, como la atestación, que pueden utilizarse en relación con la formalización de un documento público, y también independientemente de ello, por parte de un notario público no son del todo adaptables al proceso de 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 haya 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 fidedignos para determinar que sigue una trayectoria fiable[180].

134. Sin embargo, la firma electrónica segura cumpliría una función análoga a la del testigo que declara para identificar a la persona que supuestamente firma el documento. La utilización de una firma electrónica segura permitiría, sin la presencia de un testigo humano, 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 dé fe de una firma digital segura serían tal vez ínfimas, a menos que se pusiera en duda el carácter voluntario de la firma[181].

135. La legislación en vigor no ha llegado a sustituir enteramente por la firma electrónica los requisitos de atestación, 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"[182].

136. 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

---

[180] 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 también para un análisis de la labor de los controladores de la confianza de la visualización) (V. Liu y otros, "Visually sealed and digitally signed documents", Association of Computing Machinery, *ACM International Conference Proceedings Series, vol. 56;* y *Proceedings of the Twenty-seventh Australasian Conference on Computer Science*, vol. 26, (Dunedin, Nueva Zelandia, 2004) pág. 287.

[181] Véanse los análisis *Joint IDA-AGC Review of Electronic Transactions Act Stage II: Exclusions under Section 4 of the ETA*, del Organismo de Desarrollo Conjunto 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), partes quinta y octava, disponible en la sección "Publications" del sitio www.agc.gov.sg (consultado el 6 de junio de 2008).

[182] Nueva Zelandia, Ley de Operaciones Electrónicas (véase la nota 88), artículo 23.

y testigos estampan su firma electrónica segura en dicho documento electrónico[183]. 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[184]. La declaración que debe hacerse bajo juramento o promesa 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 promesa solemne, estampa a su vez en ella su firma electrónica segura[185]. 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[186].

[183] Canadá, Ley de Protección de la Información Personal y Documentos Electrónicos (2000), segunda parte, artículo 46.

[184] Canadá, Ley de Protección de la Información Personal…, artículo 45.

[185] Canadá, Ley de Protección de la Información Personal…, artículo 44.

[186] 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 Inmobiliaria, 2005), disponible en http://www.cofrestrfatir.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc (consultado el 5 de junio de 2008). Se prevé ejecutar el proyecto por etapas entre 2006 y 2009.

Segunda parte

Utilización transfronteriza de los métodos de firma y autenticación electrónicas

Índice

I. Reconocimiento jurídico de los métodos de autenticación y firma electrónicas extranjeros

137. Las incompatibilidades jurídicas y técnicas son las dos causas principales de dificultades en la utilización transfronteriza de los métodos de firma y autenticación electrónicas, en particular cuando su finalidad es sustituir una firma legalmente válida. Las incompatibilidades técnicas son las que afectan a la interoperatividad de los sistemas de autenticación. Las incompatibilidades jurídicas pueden surgir cuando las leyes de los diferentes ordenamientos estipulan diferentes requisitos en cuanto a la utilización y la validez de los métodos de firma y autenticación electrónicas.

A. Repercusión internacional de la legislación interna

138. Cuando la legislación interna admite formas electrónicas equivalentes a los métodos de autenticación basados en un soporte en papel, es posible que sean incompatibles los criterios de validez de esas formas electrónicas equivalentes. Por ejemplo, si la ley reconoce sólo las firmas digitales, no serán aceptables otras formas de firma electrónica. Puede ser que otras discrepancias en los criterios de reconocimiento de los métodos de autenticación y firma electrónicas no impidan en principio su utilización a través de las fronteras, pero el costo y las molestias resultantes de la necesidad de satisfacer los requisitos prescritos por los diversos ordenamientos tal vez reduzcan las ventajas de rapidez y eficiencia que es de esperar reporte la utilización de las comunicaciones electrónicas.

139. En las siguientes secciones se examinan las repercusiones que tienen diferentes enfoques jurídicos de la tecnología en la expansión del reconocimiento transfronterizo. También se resume el consenso internacional naciente sobre las medidas que tal vez podrían facilitar la utilización internacional de los métodos de firma y autenticación electrónicas.

1. Obstáculos internacionales creados por enfoques nacionales contrapuestos

140. Los enfoques neutrales desde el punto de vista tecnológico, en especial los que incluyen una "prueba de fiabilidad", tienden a resolver las incompatibilidades legales. Entre los instrumentos jurídicos internacionales que adoptan este enfoque figuran la Ley Modelo de la CNUDMI sobre Comercio Electrónico, en el apartado *b)* del párrafo 1 de su artículo 7, y la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, en el párrafo 3

de su artículo 9. Según este enfoque, un método de firma o autenticación electrónicas capaz de identificar al firmante e indicar su intención con respecto a la información concernida en la comunicación electrónica cumple los requisitos de la firma, siempre que satisfaga varios criterios. Atendidas todas las circunstancias del caso, incluso la existencia de un acuerdo entre el iniciador y el destinatario del mensaje de datos, hay que demostrar que el método de firma o autenticación es tan fiable como corresponde a la finalidad para la que se genera o comunica dicho mensaje. Otra posibilidad es la obligación de demostrar que ha cumplido esa finalidad por sí mismo o juntamente con otros medios probatorios.

141. Cabe sostener que el planteamiento minimalista facilita la utilización transfronteriza de la autenticación y la firma electrónicas, pues con arreglo al mismo es posible usar con validez cualquier método de firma o autenticación electrónicas para firmar o autenticar un contrato o comunicación, siempre que satisfaga las anteriores condiciones generales. Sin embargo, la consecuencia de este enfoque es que por lo general esas condiciones se confirman solamente a posteriori y no hay ninguna garantía de que un tribunal reconozca la utilización de un método determinado.

142. La utilización transfronteriza de la autenticación y las firmas electrónicas se convierte en un verdadero problema en los sistemas que prescriben imperativamente o dan preferencia a una tecnología determinada. La complejidad del problema aumenta en proporción directa al grado de regulación estatal de las firmas y la autenticación electrónicas y al grado de seguridad jurídica que la ley concede a un método o tecnología determinados. Las razones son simples: cuando la ley no atribuye validez ni presunción jurídica especial alguna a determinados tipos de firma o autenticación electrónicas, y se limita a prescribir su equivalencia general a las firmas manuscritas o a la autenticación sobre soporte de papel, los riesgos de confiar en una firma electrónica son los mismos, conforme a la legislación vigente, que el riesgo de fiarse de una firma manuscrita. En cambio, cuando la ley atribuye más presunciones legales a una firma electrónica determinada (habitualmente a las consideradas “seguras” o “avanzadas”), el grado creciente de riesgo se desplaza de una parte a la otra. Un supuesto fundamental de la legislación con orientación tecnológica específica es que ese desplazamiento general a priori del riesgo jurídico puede estar justificado por el grado de fiabilidad que ofrece una tecnología determinada, siempre que se cumplan ciertas normas y ciertos procedimientos. El reverso de este planteamiento es que una vez que se afirma la fiabilidad a priori del uso (entre otras condiciones) de una tecnología determinada, todas las demás, o incluso la misma tecnología utilizada en condiciones ligeramente diferentes, se convierten a priori en poco fiables, o al menos se hacen sospechosas a priori de falta de fiabilidad.

143. Por consiguiente, es posible que una legislación nacional con orientación tecnológica específica discrepante dificulte más que promueva la utilización de las firmas electrónicas en el comercio internacional. Ello podría suceder de dos maneras distintas pero estrechamente relacionadas.

144. Primero, si las firmas electrónicas y los proveedores de servicios de certificación que las autentican están sujetos a requisitos jurídicos y técnicos contradictorios

en diferentes ordenamientos, ello puede coartar o impedir la utilización de firmas electrónicas en muchas operaciones transfronterizas, si con esa firma es imposible satisfacer simultáneamente los requisitos de los distintos ordenamientos jurídicos.

145. Segundo, la legislación con orientación tecnológica específica, en especial la que da preferencia a las firmas digitales, lo que también sucede con el enfoque en dos fases, tiende a originar una mezcolanza de normas técnicas y requisitos de autorización contradictorios que dificulta mucho la utilización transfronteriza de firmas electrónicas. Un sistema en el que cada país prescribe sus propias normas puede también impedir que las partes concierten acuerdos de reconocimiento mutuo y certificación cruzada[187]. En efecto, un arduo problema pendiente, relativo en particular a las firmas digitales, es el del reconocimiento transfronterizo. El Grupo de Trabajo sobre la seguridad de la información y la protección de la vida privada, de la Organización de Cooperación y Desarrollo Económicos (OCDE) (en lo sucesivo Grupo de Trabajo de la OCDE) ha hecho observar que, si bien el enfoque adoptado por la mayoría de los ordenamientos jurídicos parece ser no discriminatorio, las diferencias de los requisitos a nivel nacional continuarán generando problemas de interoperatividad[188]. A los efectos del presente estudio, pueden ser significativos los siguientes puntos débiles señalados por el Grupo de Trabajo de la OCDE:

a) Interoperatividad. Se comprobó que eran frecuentes los problemas y limitaciones en cuanto a interoperatividad. En el plano técnico, aunque abundan las normas, se citó como problema la falta de normas "básicas" comunes a algunas tecnologías. En el plano jurídico/normativo, se señalaron como factores que impedían el progreso la dificultad de los responsables en comprender sus respectivos marcos de confianza mutua, incluso en los temas de asignación de responsabilidad e indemnización. Según el Grupo de Trabajo de la OCDE éste es un ámbito que parece requerir un examen y análisis más a fondo con miras a elaborar tal vez instrumentos comunes que sean útiles a los ordenamientos jurídicos al objeto de lograr el grado de interoperatividad deseado para una aplicación o sistema determinados;

b) Reconocimiento de los servicios de autenticación extranjeros. Según el Grupo de Trabajo de la OCDE, la labor se ha centrado en el establecimiento de servicios nacionales. En consecuencia, los mecanismos de reconocimiento de los servicios de autenticación extranjeros no se han desarrollado por lo general muy satisfactoriamente. En estas condiciones, el mencionado Grupo de Trabajo señala que éste parece ser un ámbito en que sería de utilidad proseguir la tarea. Dado que los trabajos en este terreno guardarían estrecha relación con la cuestión más general de la interoperatividad, estos temas podrían combinarse;

---

[187] Baker y Yeo, "Background and issues concerning authentication ...".

[188] Organización de Cooperación y Desarrollo Económicos, Grupo de Trabajo sobre la seguridad de la información y la protección de la vida privada, "*The Use of Authentication across Borders in OECD Countries*" (DSTI/ICCP/REG(2005)4/FINAL), disponible en http://www.oecd.org/dataoecd/1/10/35809749.pdf, (consultado el 6 de junio de 2008).

c) Aceptación de credenciales[189]. En algunos casos, se señaló como impedimento para la interoperatividad la aceptación de las credenciales emitidas por otras entidades. A este respecto, el Grupo de Trabajo de la OCDE sugiere que podría considerarse la posibilidad de establecer una serie de prácticas óptimas o directrices relativas a la emisión de credenciales con fines de autenticación. Es posible que en diversos ordenamientos jurídicos estén ya en curso trabajos sobre este tema que podrían constituir una útil aportación a eventuales iniciativas del Grupo de Trabajo de la OCDE sobre el particular;

d) Se utiliza una amplia variedad de métodos de autenticación. El Grupo de Trabajo de la OCDE constató que prácticamente en todos los Estados Miembros de la Organización se hacía uso de una amplia variedad de soluciones al tema de la autenticación. Los métodos van desde el uso de contraseñas, por una parte, hasta elementos simbólicos, firmas digitales y datos biométricos, por otra. Según sea la aplicación, y los correspondientes requisitos, los métodos pueden utilizarse solos o en combinación. Muchos observadores podrían considerar que ello es positivo, pero la información reunida en el estudio del Grupo de Trabajo de la OCDE da a entender que la gama de posibilidades es tan amplia que existe el riesgo de que los proveedores y usuarios de aplicaciones se vean sumidos en la mayor perplejidad al decidir qué método es el apropiado para sus necesidades. Según el mencionado Grupo de Trabajo, esto parecería indicar que sería en cierto modo ventajoso establecer un instrumento de referencia para evaluar los diversos métodos de autenticación y el grado en que sus características responden a las necesidades constatadas por los proveedores o los usuarios de aplicaciones.

146. La confianza en la utilización de métodos de firma y autenticación electrónicas podría incrementarse con la adopción de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales y la aplicación de su enfoque de neutralidad tecnológica a las firmas y la autenticación electrónicas. Ahora bien, es poco realista esperar que ello obviaría por completo la necesidad de una solución armonizada para abordar normativas jurídicas y técnicas incompatibles. Es posible que muchos países sigan prescribiendo el uso de métodos específicos de autenticación en ciertos tipos de operación. También puede ser que algunos países estimen necesaria orientación más concreta para aquilatar la fiabilidad de los métodos de firma y autenticación, en particular los extranjeros, y su equivalencia a los métodos utilizados o al menos conocidos en el país.

2. Gestación de un consenso

147. La divergencia de normativas que se ha dado a nivel internacional es probablemente resultado de una combinación de factores, en grados variables. Como se

[189] Una credencial es un elemento simbólico dado para probar que una persona o un aparato determinado se ha sometido a un proceso de autenticación. Las credenciales vinculadas al usuario son esenciales a efectos de identificación. Las credenciales al portador pueden ser suficientes para algunas formas de autorización. Como ejemplos cabe citar un permiso de conducir válido, el número de seguridad social u otro número identificador de una persona, o bien las tarjetas con microcircuito (Centro para la Democracia y la Tecnología, "Privacy principles for authentication systems", disponible en http://www.cdt.org/privacy/authentication/030513interim.shtml, (consultado el 5 de junio de 2008)).

ha señalado anteriormente (véanse los párrs. 2 a 6 *supra*) algunos países tienden a establecer requisitos más estrictos y particularizados en lo que respecta a las firmas y los documentos, mientras que otros centran su interés en la intención de la parte firmante y permiten una extensa variedad de formas de probar la validez de las firmas. Estas diferencias generales suelen traslucirse en la legislación concreta relativa a los métodos de autenticación y firma electrónicas (véanse los párrs. 91 a 119 *supra*). Otra causa de incoherencia es resultado del grado variable de ingerencia de las autoridades nacionales en los aspectos técnicos de dichos métodos. Algunos países tienden a desempeñar un papel directo en el establecimiento de normas sobre nuevas tecnologías, posiblemente en la creencia de que ello confiere una ventaja competitiva a la industria nacional[190].

148. La divergencia de las normativas puede también obedecer a diferentes hipótesis sobre la forma en que cristalizarán las tecnologías de autenticación. En uno de esos supuestos, el llamado "paradigma universal de autenticación"[191], se da por sentado que la finalidad principal de las tecnologías de autenticación será verificar las identidades y características entre personas que no tienen ninguna relación anterior entre sí y cuyo uso común de la tecnología no es el objeto del acuerdo contractual. Por tanto, lo que debe hacer la tecnología de autenticación o firma es confirmar la identidad u otras características de una persona a un número de personas potencialmente ilimitado y para un número de fines potencialmente ilimitado. Este modelo hace hincapié en la importancia de las normas técnicas y de los requisitos operativos de los proveedores de servicios de certificación en el caso de terceros en los que se deposita confianza. Otro marco hipotético, el llamado "paradigma de autenticación limitado" parte del supuesto de que el principal uso de las tecnologías de autenticación y firma será verificar las identidades y características entre personas cuyo uso común de la tecnología se realiza con sujeción a acuerdos contractuales[192]. Por consiguiente, lo que debe hacer la tecnología de autenticación es confirmar la identidad u otras características del poseedor del certificado sólo para una serie de fines concretamente especificados y dentro de una colectividad definida de partes potencialmente confiantes que se someten a condiciones comunes para el uso de la tecnología. Este modelo hace hincapié en el reconocimiento jurídico de los acuerdos contractuales.

149. Pese a estas discrepancias, algunas de las cuales aún predominan, las constataciones del Grupo de Trabajo de la OCDE[193] dan a entender que parece existir ahora un creciente consenso internacional sobre los principios básicos que deben regir el comercio electrónico y en particular la firma electrónica. Para el presente estudio son de especial interés las constataciones siguientes:

a) Enfoque no discriminatorio de las firmas y servicios "extranjeros". Los marcos legislativos no niegan efectividad jurídica a las firmas provenientes de servicios con sede en otros países siempre que esas firmas se hayan creado en las mismas

[190] Baker y Yeo, "Background and issues concerning authorization ...".

[191] Baker y Yeo, "Background and issues concerning authorization ...".

[192] Baker y Yeo, "Background and issues concerning authorization ...".

[193] Organización de Cooperación y Desarrollo Económicos, "*The Use of Authentication across Borders in OECD Countries...*".

condiciones que aquellas a las que se ha dado efecto legal en el ámbito interno. En tal caso, el enfoque parece ser no discriminatorio, siempre que se satisfagan los requisitos nacionales o su equivalente. Ello concuerda con las constataciones de anteriores estudios sobre la autenticación efectuados por el Grupo de Trabajo de la OCDE;

b) Neutralidad tecnológica. Aunque prácticamente todos los que respondieron a la encuesta indicaron que su marco legislativo y reglamentario de los servicios de autenticación y firmas electrónicas era tecnológicamente neutral, la mayoría señaló que, cuando se trataba de aplicaciones electrónicas en la administración pública o cuando se requería la máxima seguridad jurídica de la firma electrónica, se estipulaba la utilización de una infraestructura de clave pública (ICP). En esas condiciones, aunque los marcos legislativos pueden ser tecnológicamente neutros, las decisiones de política parecen exigir la especificación de la tecnología;

c) Predominio de la ICP. Según el Grupo de Trabajo de la OCDE, la ICP parece ser el método de autenticación preferido cuando se requieren pruebas sólidas de la identidad y una gran seguridad jurídica de la firma electrónica. Se utiliza en determinadas "comunidades de intereses" cuando todos los usuarios parecen tener una relación comercial previa de alguna forma. El uso de tarjetas con microcircuito habilitadas para la ICP y la integración de funciones de certificación digital en los programas informáticos de aplicaciones han hecho que el empleo de este método sea menos complicado para los usuarios. Sin embargo, se reconoce en general que la ICP no es necesaria para todas las aplicaciones y que la selección de los métodos de autenticación debe efectuarse en función de su adecuación a los fines para los que se utilicen.

150. Además, el Grupo de Trabajo de la OCDE constató que los sistemas reguladores de todos los países estudiados tenían establecida alguna forma de marco legislativo o reglamentario que regulara el efecto jurídico de las firmas electrónicas a nivel nacional. El Grupo de Trabajo comprobó que, si bien los detalles de la legislación podían diferir de unos ordenamientos jurídicos a otros, parecía ser discernible un enfoque uniforme en el sentido de que la mayoría de las leyes internas tenía como base marcos internacionales o transnacionales ya existentes (por ejemplo, la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas y la Directiva 1999/93/CE del Parlamento Europeo y del Consejo sobre un marco comunitario para las firmas electrónicas[194]).

151. Los puntos esenciales de esta gestación de consenso se han vuelto a enunciar en la Recomendación sobre autenticación electrónica, aprobada por el Consejo de la OCDE el 12 de junio de 2007, en la que, entre otras cosas, se invita a los Estados a:

a) Trabajar para lograr el establecimiento de enfoques neutrales desde el punto de vista tecnológico a fin de conseguir una autenticación electrónica nacional y transfronteriza eficaz de las personas y las entidades;

b) Fomentar el desarrollo, suministro y la utilización de productos y servicios de autenticación electrónica que incorporen buenas prácticas comerciales, incluidas las salvaguardias técnicas y no técnicas para satisfacer las necesidades de los participantes,

[194] *Diario Oficial de las Comunidades Europeas*, L 13/12, 19 de enero de 2000.

en particular con respecto a la seguridad y la protección de la información e identidad relativas a su esfera privada;

c) Tanto en el sector privado como en el público, fomentar la compatibilidad comercial y jurídica y la interoperabilidad técnica de los sistemas de autenticación, a fin de facilitar las interacciones y transacciones intersectoriales e interjurisdiccionales en línea, así como para asegurarse de que los productos y servicios de autenticación pueden movilizarse tanto a nivel nacional como internacional; y

d) Adoptar medidas para concienciar a todos los participantes, en particular a los de las economías de los países que no son Miembros, sobre los beneficios de la utilización de medios electrónicos de autenticación a nivel nacional e internacional[195].

152. Estas recomendaciones son perfectamente compatibles con el enfoque global adoptado por la CNUDMI en el ámbito del comercio electrónico (por ejemplo, la facilitación en lugar de la regulación, neutralidad desde el punto de vista tecnológico, el respeto de la libertad contractual, el principio de no discriminación). No obstante, existen varias cuestiones jurídicas que es necesario examinar para facilitar la utilización de métodos de autenticación y firma electrónicas en un contexto internacional o transfronterizo.

B. Criterios de reconocimiento de los métodos extranjeros de autenticación y firma electrónicas

153. Como se ha indicado anteriormente, uno de los principales obstáculos a la utilización transfronteriza de las firmas y la autenticación electrónicas viene siendo la falta de interoperatividad, debida a normas contradictorias o discrepantes, o bien a su aplicación inconsecuente. Se han creado varios foros para promover una ICP normalizada e interoperativa como fundamento de la seguridad de las operaciones en las aplicaciones del comercio electrónico. Entre ellos figuran organizaciones

[195] *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*, (París, junio de 2007) disponible en http://www.oecd.org/dataoecd/32/45/38921342.pdf, (consultado el 6 de junio de 2008).

intergubernamentales[196] y mixtas del sector público y el sector privado[197] a nivel mundial[198] o regional.

154. El objetivo de algunos de estos trabajos es establecer normas técnicas sobre la presentación de la información necesaria para cumplir ciertos requisitos legales[199]. Pero, en gran medida, esta importante labor se ocupa sobre todo de los aspectos técnicos y no de las cuestiones jurídicas, por lo que se sitúa fuera del ámbito del presente estudio. En consecuencia, el análisis efectuado en las secciones siguientes se centra en los requisitos jurídicos formales y sustantivos para el reconocimiento transfronterizo de las firmas electrónicas.

---

[196] En la región de Asia y el Pacífico, el foro de la Asociación de Cooperación Económica en Asia y el Pacífico (APEC) ha elaborado el documento "Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction eCommerce" (Grupo de Tareas sobre seguridad electrónica, Grupo de Trabajo de la APEC sobre telecomunicaciones e información, diciembre de 2004) (disponible en http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf (el original se puede consultar en la Secretaría)). La finalidad de esas directrices es facilitar el establecimiento de sistemas potencialmente interoperativos así como el examen de la interoperatividad de sistemas existentes. Las directrices tratan solamente las clases o tipos de certificados utilizados en el comercio electrónico transnacional. No tienen por objeto otros certificados ni pretenden limitar los sistemas solamente a la emisión de los certificados que en ellas se contemplan.

[197] En la Unión Europea, la Junta de Normalización en materia de Tecnología de la Información y las Comunicaciones (TIC) creó en 1999 la Iniciativa europea de normas para firmas electrónicas (EESSI) dirigida a coordinar las actividades de normalización en apoyo de la aplicación de la Directiva 1999/93/CE de la Unión Europea, referente a las firmas electrónicas. La Junta de Normalización en materia de TIC es una iniciativa del Comité Europeo de Normalización (CEN), creado por organizaciones de normalización nacionales y dos organizaciones sin fines de lucro: el Comité Europeo de Normalización Electrotécnica y el Instituto Europeo de Normas de Telecomunicación (ETSI). La EESSI ha elaborado varias normas para promover la interoperatividad, pero su aplicación es lenta, supuestamente a causa de su complejidad (Paolo Balboni, "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information and Communications Technology Law*, vol. 13, Nº 3, 2004, págs. 211 a 242.

[198] Por ejemplo, la Organization for the Advancement of Structured Information Standards (OASIS), consorcio internacional sin fines lucrativos fundado en 1993 para fomentar el desarrollo, la convergencia y la adopción de normas para el comercio electrónico. La OASIS ha establecido un comité técnico sobre ICP, formado por usuarios de ICP, vendedores y expertos, encargado de estudiar las cuestiones relativas a la propagación de la tecnología de certificación digital. Dicho comité técnico ha preparado un plan de acción que prevé, entre otras cosas, la elaboración de directrices o perfiles específicos que describan la forma en que las normas deben utilizarse en determinadas aplicaciones para conseguir la interoperatividad en materia de ICP, establecer nuevas normas cuando sea necesario, y prever pruebas de interoperatividad y actos de comprobación (OASIS, comité técnico sobre ICP, "plan de acción ICP", (febrero de 2004), http://www.oasis-open.org/committees/pki/pkiactionplan.pdf (consultado el 6 de junio de 2008)).

[199] Por ejemplo, el ETSI ha establecido una norma (TS 102 231) para instaurar una estructura no jerárquica que, entre otras cosas, permite abordar el reconocimiento cruzado de dominios de ICP y, en consecuencia, de la validez de los certificados. En lo fundamental, la norma TS 102 231 especifica pautas para la presentación de información sobre la situación de un proveedor de servicios de certificación (llamado "proveedor de servicios de confianza mutua"). Reviste la forma de una lista firmada, la "lista de situación de los servicios de confianza mutua", como base para la presentación de esa información. La lista de situación de servicios de confianza mutua especificada por el ETSI satisface el requisito de ofrecer pruebas sobre si el proveedor de un servicio de confianza mutua actúa o actuaba bajo la aprobación de un sistema reconocido cualquiera bien en el momento de prestarse el servicio, o en el momento en que se realizó una operación confiando en ese servicio. Para cumplir este requisito la lista de situación del servicio de confianza mutua ha de contener información por la cual sea posible determinar si el gestor del sistema conoció la intervención del proveedor de servicios de certificación en el momento de la operación y, en tal caso, cuál era la situación del servicio (es decir, si estaba aprobado, suspendido, cancelado o revocado). Por consiguiente, la lista de situación del servicio de confianza mutua contemplada en la norma técnica TS 102 231 del ETSI ha de contener no sólo la situación actual del servicio, sino además la historia de su situación. En consecuencia, la lista se convierte en una combinación de servicios válidos ("lista blanca") y servicios cancelados o revocados ("lista negra") (véase http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc, consultado el 6 de junio de 2008).

1. Lugar de origen, reciprocidad y validación a nivel nacional

155. El lugar de origen es un factor clásico a la hora de otorgar reconocimiento jurídico a los documentos o escritos del extranjero. Esto se hace habitualmente sobre la base de la reciprocidad, de forma que se concede efecto en el ámbito nacional propio a las firmas y certificados de un país determinado en la medida en que el otro país da efecto legal a las firmas y certificados nacionales. Otro factor conexo es supeditar el efecto interno de la firma o el certificado de origen extranjero a alguna forma de validación o reconocimiento por parte de un proveedor de servicios de certificación, una autoridad de certificación o una entidad reguladora nacional. En algunos de ellos se combinan todos estos factores[200].

156. No es corriente que las leyes internas denieguen expresamente el reconocimiento legal de las firmas o certificados extranjeros, lo que puede confirmar su carácter en apariencia no discriminatorio. Sin embargo, en la práctica, son muchos los regímenes de reconocimiento que suelen tener algún efecto discriminatorio, incluso no premeditado. Por ejemplo, la Directiva de la Unión Europea sobre la firma electrónica proscribe en general la discriminación de los certificados extranjeros que reúnan las condiciones (es decir, las firmas digitales basadas en una ICP). Sin embargo, esto redunda sobre todo en favor de los certificados emitidos por los proveedores de servicios de certificación establecidos en el territorio de los Estados miembros de la Unión Europea. Un proveedor de dichos servicios establecido en un tercer país tiene tres opciones para conseguir el reconocimiento de su certificado en la misma: cumplir los requisitos establecidos en la Directiva de la Unión Europea sobre la firma electrónica y obtener acreditación en el marco de un sistema establecido en un Estado miembro; concertar una certificación cruzada con un proveedor de servicios de certificación establecido en un Estado miembro de la comunidad europea; u operar al amparo de un reconocimiento general otorgado a nivel de un acuerdo internacional[201]. Por la forma en que la Directiva Europea regula los aspectos internacionales se colige que uno de sus objetivos era asegurar a los proveedores de servicios de certificación de la Unión Europea condiciones de acceso a los mercados extranjeros[202]. Al acumular el requisito

[200] En la Argentina, por ejemplo, se reconocen los certificados y las firmas electrónicas de origen extranjero siempre que exista un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o sean "reconocidos por un certificador licenciado en el país, y este reconocimiento sea validado por la autoridad de aplicación" (véase la Ley de firma digital (2001), art. 16).

[201] En efecto, según lo dispuesto en el artículo 7 de la Directiva, los Estados miembros de la Unión Europea sólo deben velar por que los certificados expedidos por un proveedor de servicios de certificación establecido en un tercer país sean reconocidos como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad siempre que: *a)* el proveedor de servicios de certificación "cumpla los requisitos establecidos en la presente Directiva y haya sido acreditado en el marco de un sistema voluntario de acreditación establecido en un Estado miembro"; o *b)* un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones de la presente Directiva "avale" el certificado; o bien *c)* el certificado o el proveedor de servicios de certificación "estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales".

[202] El interés por asegurar el acceso de los proveedores de servicios de certificación europeos a los mercados extranjeros se desprende claramente de la formulación del párrafo 3 del artículo 7 de la Directiva, el cual estipula que "cuando la Comisión sea informada de cualquier dificultad encontrada por las empresas comunitarias en relación con el acceso al mercado en terceros países, podrá en caso necesario presentar propuestas al Consejo para obtener un mandato adecuado para la negociación de derechos comparables para las empresas comunitarias en dichos terceros países".

de equivalencia sustancial a las normas de la Unión Europea más el requisito adicional de "acreditación en el marco de un sistema establecido en un Estado miembro", la Directiva de la Unión Europea sobre la firma electrónica exige de hecho que los proveedores de servicios de certificación extranjeros cumplan el régimen propio de partida más el de la Unión Europea, lo cual es un nivel más elevado que el exigido a los proveedores de servicios de certificación acreditados en un Estado miembro de la Unión[203].

157. El artículo 7 de la Directiva de la Unión Europea se ha aplicado con algunas variantes[204]. Irlanda y Malta, por ejemplo, reconocen las firmas digitales extranjeras (certificados reconocidos, según la terminología de la Unión) como equivalentes a las firmas nacionales siempre que satisfagan los demás requisitos jurídicos. En otros casos el reconocimiento está sujeto a verificación nacional (Austria, Luxemburgo) o a una decisión de una autoridad nacional (Estonia, Polonia, República Checa). Esta tendencia a insistir en alguna forma de verificación nacional, justificada en general por una legítima preocupación acerca del grado de fiabilidad de los certificados extranjeros, conduce en la práctica a un sistema de discriminación de los certificados extranjeros por razón de su origen geográfico.

2. Equivalencia sustancial

158. En consonancia con una vieja tradición, la CNUDMI declinó respaldar consideraciones de tipo geográfico a la hora de proponer factores para el reconocimiento de los certificados y las firmas electrónicas extranjeros. En efecto, el párrafo 1 del artículo 12 de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas estipula taxativamente que, al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, "no se tomará en consideración" ni "el lugar geográfico en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica" ni "el lugar geográfico en que se encuentre el establecimiento del expedidor o firmante".

159. El propósito del párrafo 1 del artículo 12 de la Ley Modelo de la UNCITRAL sobre las Firmas Electrónicas es dar reflejo al principio fundamental de que el lugar de origen no debe ser en modo alguno, de por sí, un factor determinante al decidir si los certificados o las firmas electrónicas de origen extranjero deben reconocerse susceptibles de producir efectos jurídicos, o en qué medida los producen. La determinación de si un certificado o una firma electrónica es susceptible de eficacia jurídica, o en qué medida lo es, debe depender de su fiabilidad técnica y no del lugar de su expedición. En algunos regímenes nacionales, por ejemplo en la Ley 2000 de los Estados Unidos sobre las firmas electrónicas en el comercio mundial y nacional, existen también disposiciones no discriminatorias similares a las del artículo 12 de la Ley Modelo sobre

[203] Jos Dumortier y otros, "The legal and market aspects of electronic signatures", Estudio para la Dirección General de Sociedad de la Información de la Comisión Europea, Katholieke Universiteit Leuven, 2003, pág. 58.

[204] Jos Dumortier y otros, "The legal and market aspects of electronic signatures"..., págs. 92 a 94.

las Firmas Electrónicas[205]. Tales disposiciones estipulan que el lugar de origen, de por sí, no debe ser un factor al determinar si los certificados o las firmas electrónicas extranjeros deben reconocerse como susceptibles de eficacia jurídica en un Estado promulgante, o en qué medida los producen. Dichas disposiciones reconocen que la efectividad jurídica de un certificado o una firma electrónica debe depender de su fiabilidad técnica[206].

160. En lugar de los factores geográficos, la Ley Modelo establece una prueba de equivalencia sustancial entre los grados de fiabilidad ofrecidos por los certificados y firmas en cuestión. En consecuencia, si el certificado extranjero expedido presenta "un grado de fiabilidad sustancialmente equivalente" al de un certificado expedido en el Estado promulgante, tendrá "los mismos efectos jurídicos". De igual modo, una firma electrónica creada o utilizada fuera del país "producirá los mismos efectos jurídicos" que una firma electrónica creada o utilizada en el país "si presenta un grado de fiabilidad sustancialmente equivalente". La equivalencia entre los grados de fiabilidad presentados por los certificados y firmas nacionales y extranjeros ha de ser determinada en conformidad con normas internacionales reconocidas y cualquier otro factor pertinente, en particular un acuerdo entre las partes para utilizar ciertos tipos de firmas o certificados electrónicos, a no ser que el acuerdo carezca de validez o efectividad con arreglo al derecho aplicable.

161. La Ley Modelo no prescribe ni propugna convenios de reciprocidad. En efecto, la ley Modelo "no prevé nada en concreto" en cuanto a las técnicas jurídicas mediante las cuales un Estado promulgante pudiera reconocer por adelantado la fiabilidad de los certificados y las firmas que cumpliesen la legislación de un país extranjero (por ejemplo, una declaración unilateral o un tratado)[207]. Los posibles métodos para alcanzar este resultado que se mencionaron al elaborar la Ley Modelo fueron, por ejemplo, el reconocimiento automático de las firmas que cumplieran las leyes de otro Estado si las leyes del Estado extranjero exigían un nivel de fiabilidad al menos equivalente al requerido para las firmas nacionales equivalentes. Otras técnicas legales mediante las cuales un Estado promulgante pudiera reconocer por anticipado la fiabilidad de los certificados y firmas extranjeros podrían ser declaraciones unilaterales o tratados[208].

---

[205] Código de los Estados Unidos, título 15, capítulo 96, artículo 7031 (Principios que rigen la utilización de las firmas electrónicas en las operaciones internacionales).

[206] *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas*..., segunda parte, párr. 83.

[207] Ibíd., párr. 157.

[208] Véase el informe del Grupo de Trabajo sobre comercio electrónico acerca de la labor de su 37º período de sesiones (A/CN.9/483, párrs. 39 y 42).

II. Métodos y criterios para establecer la equivalencia jurídica

162. Como se indicó antes, en el estudio realizado por el Grupo de Trabajo de la Organización de Cooperación y Desarrollo Económicos (OCDE) sobre la seguridad de la información y la protección de la vida privada se determinó que, en la mayoría de los marcos legislativos, como mínimo no se discriminaba en principio a los métodos de firma y autenticación electrónicas de origen extranjero –siempre que se cumplieran requisitos nacionales o sus equivalentes, en el sentido de que no restaran eficacia jurídica a las firmas relacionadas con servicios originarios de los países– y que esas firmas se hubieran creado en las mismas condiciones que las reconocidas con arreglo al derecho interno[209]. Sin embargo, el Grupo de Trabajo de la OCDE sobre la seguridad de la información y la protección de la vida privada señaló también que los mecanismos para reconocer los servicios extranjeros de autenticación no estaban en general desarrollados, y consideró que sería útil ocuparse en el futuro de este aspecto. Habida cuenta de que toda labor en este ámbito guardaría estrecha relación con el tema general de la interoperabilidad, el Grupo de Trabajo de la OCDE señaló que estos temas podrían refundirse. El Grupo de Trabajo propuso que se elaborara un conjunto de prácticas óptimas o directrices. Más recientemente, la OCDE señaló también que los mecanismos para reconocer los servicios extranjeros de autenticación se han desarrollado "si bien la experiencia en materia de aplicaciones interjurisdiccionales es escasa". Por otra parte, "las jurisdicciones necesitan algunos medios para evaluar los marcos de confianza de sus asociados". A pesar de que la OCDE expresó su deseo de que sus propias directrices y el marco que ofrecen sirvan de ayuda a este respecto, señaló que "es necesario llevar a cabo una labor más amplia sobre esta cuestión"[210]. En las secciones siguientes se examinan las disposiciones y los mecanismos jurídicos para la interoperabilidad internacional y los factores que determinan la equivalencia de los regímenes de responsabilidad. Se centran principalmente en las cuestiones que plantea la utilización internacional de los métodos de firma y autenticación electrónicas respaldados con certificados expedidos por un tercer prestador de servicios de certificación en quien se confía, en particular las firmas digitales consignadas por medio de una infraestructura de clave pública (ICP), porque es más probable que surjan dificultades jurídicas en relación con la utilización transfronteriza de los métodos de firma y autenticación electrónicas que requieran la participación de terceros en el trámite de firma o autenticación.

[209] Organización de Cooperación y Desarrollo Económicos, "*The Use of Authentication across Borders in OECD Countries...*".

[210] *OECD Recommendation on Electronic Authentication...*, pág. 27.

A. Tipos y mecanismos de reconocimiento recíproco

163. La carga suplementaria que imponen al prestador de servicios de certificación extranjero los requisitos nacionales determinados por la tecnología puede convertirse en obstáculo al comercio internacional[211]. Por ejemplo, las leyes relativas a los medios por los que las autoridades nacionales reconocen firmas y certificados electrónicos extranjeros podían constituir discriminación contra las empresas extranjeras. Hasta ahora, todos los poderes legislativos que han examinado esta cuestión han incluido en sus leyes alguna prescripción relativa a las normas que observa el prestador de servicios de certificación extranjero, por lo que esta cuestión se halla indisolublemente ligada a la más amplia de las posibles diferencias entre las normas vigentes en los países. Al mismo tiempo, la legislación puede imponer otras limitaciones geográficas o de procedimiento que impidan el reconocimiento transfronterizo de las firmas electrónicas.

164. En ausencia de una ICP internacional, podrían plantearse varios problemas con respecto al reconocimiento de certificados por las autoridades de certificación de países extranjeros. El reconocimiento de los certificados extranjeros se realiza a menudo mediante un método llamado "certificación recíproca". En tal caso, es necesario que autoridades de certificación fundamentalmente equivalentes (o autoridades de certificación dispuestas a asumir ciertos riesgos con respecto a los certificados expedidos por otras autoridades de certificación) reconozcan los servicios prestados por cada cual, de manera que sus usuarios respectivos puedan comunicarse entre sí con mayor eficacia y más confianza en la fiabilidad del certificado que se expida. Podrán plantearse problemas jurídicos con respecto a la certificación recíproca o el encadenamiento de certificados cuando haya múltiples políticas de seguridad, por ejemplo el de determinar quién ha tenido una conducta indebida que ha causado una pérdida y en cuyas declaraciones confiaba el usuario.

1. Reconocimiento recíproco

165. El reconocimiento recíproco es un arreglo de interoperabilidad, en virtud del cual la parte que confía y que se encuentre en la zona abarcada por una ICP puede utilizar información autorizada correspondiente a la zona de cobertura de otra ICP para autenticar datos en la zona abarcada por la primera ICP[212]. Ello suele ser resultado de un trámite oficial de concesión de licencia o acreditación en el ámbito de otra ICP, o de una auditoría oficial del prestador de servicios de certificación representativo de la

[211] Véase Alliance for Global Business, "A discussion paper on trade-related aspects of electronic commerce in response to the WTO´s e-commerce work programme", abril de 1999, pág. 29 (disponible en http://www.biac.org/statements/iccp/AGBtoWTOApril1999.pdf, consultado el 6 de junio de 2008).

[212] El concepto de reconocimiento recíproco fue elaborado en 2000 por el entonces llamado Electronic Authentication Task Group del entonces llamado Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (véase la publicación Nº 202-TC-01.2 del Foro de Cooperación Económica de Asia y el Pacífico titulada "*Electronic Authentication: Issues Relating to Its Selection and Use*", (2002), disponible en http://www.apec.org/apec/publications/all_publications/telecommunications.html (consultado el 6 de junio de 2008).

zona de la ICP correspondiente[213]. La responsabilidad de confiar en una zona de ICP extranjera recae en la parte que confía o en el propietario de la aplicación o el servicio, antes que en el prestador de servicios de certificación a quien se haya encomendado directamente la parte que confía.

166. El reconocimiento recíproco se produciría característicamente en el plano de la ICP antes que en el de un prestador de servicios de certificación determinado. Así pues, cuando una ICP reconoce a otra, también reconoce automáticamente a todos los prestadores de servicios de certificación acreditados en el marco de esta última. El reconocimiento se basaría en la evaluación del trámite de acreditación de la otra ICP antes que en la de cada prestador de servicios de certificación acreditado por esa ICP. Cuando las ICP expiden múltiples tipos de certificados, el trámite de reconocimiento recíproco supone determinar una clase de certificados aceptables para su utilización en los dos ámbitos, y basar la evaluación en esa clase de certificados.

167. El reconocimiento recíproco entraña cuestiones de interoperabilidad técnica únicamente en el plano de la aplicación; es decir, la aplicación debe poder procesar el certificado extranjero y entrar en el sistema de directorios de la zona de ICP extranjera para validar la condición jurídica del certificado extranjero. Cabe señalar que, en la práctica, los prestadores de servicios de certificación expiden certificados con diversos niveles de fiabilidad en función de las finalidades para las que se propongan utilizarlos sus clientes. Según su nivel respectivo de fiabilidad, los certificados y las firmas electrónicas pueden surtir efectos jurídicos distintos, tanto en el país como en el extranjero. Por ejemplo, en determinados países, incluso los certificados a los que a veces se denomina "de bajo nivel" o "de bajo valor" podrían surtir efectos jurídicos en determinadas circunstancias (por ejemplo, cuando las partes hubieran acordado contractualmente utilizarlos) (véase *infra*, párrs. [42 a 50]). Por ello, lo que se debe establecer es la equivalencia entre certificados funcionalmente comparables.

168. Como se señaló *supra*, a efectos del reconocimiento recíproco la decisión de confiar en un certificado extranjero corresponde a la parte que confía y no a su prestador de servicios de certificación. Ello no entraña necesariamente un contrato o acuerdo entre dos dominios de ICP. Tampoco se requiere una exposición detallada de las políticas de certificación[214] y las declaraciones de prácticas en materia de certificación[215], porque la parte que confía decide si aceptar o no el certificado extranjero dependiendo de si éste ha sido expedido por un prestador de servicios de certificación extranjero fiable. Se considera que este prestador de servicios de certificación lo es si le ha otorgado licencia o acreditado un órgano oficial de concesión de licencias o acreditación, o si ha sido sometido a auditoría por un tercero independiente digno de confianza. La parte que confía adopta unilateralmente una decisión informada basándose en la política

[213] Definición basada en la labor del Grupo de trabajo sobre telecomunicaciones e información del Foro de Cooperación Económica de Asia y el Pacífico, Grupo de trabajo sobre autenticación electrónica.

[214] Por política de certificación se entiende un determinado conjunto de normas en las que se indica la aplicabilidad de un certificado a una comunidad en particular y/o a una clase de aplicación con prescripciones comunes en materia de seguridad.

[215] Por declaración de prácticas de certificación se entiende una exposición de las prácticas que utiliza un prestador de servicios de certificación para expedir los certificados.

de certificación o en la declaración de prácticas de certificación del dominio de ICP extranjero.

2. Certificación recíproca entre infraestructuras de clave pública

169. La certificación recíproca es la práctica de reconocer la clave pública de otro prestador de servicios de certificación por referencia a un nivel convenido de confianza, habitualmente en virtud de un contrato. Básicamente da lugar a que dos dominios de ICP se fusionen (total o parcialmente) en uno mayor. Para los usuarios de uno de los prestadores de servicios de certificación, los del otro prestador de esos servicios son sencillamente firmantes en el marco de la ICP ampliada.

170. La certificación recíproca supone la interoperabilidad técnica y la armonización de las políticas de certificación y las declaraciones de prácticas de certificación. La armonización de las políticas, consistente en la armonización de las políticas de certificación y las declaraciones de prácticas de certificación, resulta necesaria para asegurar que los dominios de ICP sean compatibles tanto en términos de sus operaciones de gestión de certificados (o sea, su expedición, suspensión y revocación) como en su observancia de prescripciones operativas y de seguridad análogas. También es importante el grado de aplicación del régimen de la responsabilidad. Este aspecto es muy complejo, porque los documentos en cuestión suelen ser voluminosos y se ocupan de una gran diversidad de cuestiones.

171. La certificación recíproca resulta especialmente apropiada en los modelos empresariales relativamente cerrados, por ejemplo, si ambos dominios de ICP comparten un conjunto de aplicaciones y servicios, como correo electrónico o aplicaciones financieras. La existencia de sistemas técnicamente compatibles y operables, políticas congruentes y las mismas estructuras jurídicas facilitaría enormemente la certificación recíproca.

172. La certificación unilateral (en la que un dominio de ICP confía en otro pero no a la inversa) no es habitual. El dominio de ICP que confía debe velar unilateralmente por que sus políticas sean compatibles con las del dominio de ICP objeto de su confianza. Su utilización parece limitarse a las aplicaciones y servicios en que la confianza necesaria para la operación de que se trate es unilateral, por ejemplo, una aplicación en que el comerciante debe demostrar la identidad al cliente antes de que éste presente información confidencial.

B. Equivalencia de las normas de conducta y los regímenes de responsabilidad

173. Tanto si la utilización internacional de métodos de firma y autenticación electrónicas se basa en un plan de reconocimiento recíproco como si recurre a la certificación recíproca, toda decisión de reconocer íntegramente a una ICP o a uno

o más prestadores de servicios de certificación extranjeros, o de establecer niveles equivalentes entre categorías de certificados expedidos en el marco de distintas ICP, presupone una evaluación de la equivalencia entre las prácticas de certificación y los certificados nacionales y extranjeros[216]. Desde la perspectiva jurídica, ello requiere examinar la equivalencia de tres elementos principales: equivalencia en valor jurídico; equivalencia en obligaciones legales y equivalencia en régimen de responsabilidad.

174. La equivalencia en valor jurídico significa atribuir a un certificado y firma extranjeros el mismo efecto jurídico de su equivalente nacional. El efecto jurídico nacional resultante vendrá determinado en lo esencial por el valor que se atribuya en el derecho interno a los métodos de firma y autenticación electrónicas que ya se analizaron (véase *supra*, párrafos 115 a 119). Reconocer la equivalencia de las obligaciones legales y los regímenes de responsabilidad entraña la constatación de que las obligaciones impuestas a las partes que actúen conforme a un régimen de ICP corresponden en lo sustancial a las previstas conforme al régimen interno, y de que su responsabilidad por el incumplimiento de estas obligaciones es sustancialmente la misma.

175. La responsabilidad en el contexto de las firmas electrónicas puede plantear distintas cuestiones en función de la tecnología y la infraestructura de certificación utilizadas. Pueden surgir cuestiones complejas, en particular en los casos en que se encargue de la certificación un tercero especializado, como un prestador de servicios de certificación. En este caso, habrá en lo esencial tres partes, que serán el prestador de servicios de certificación, el firmante y el tercero que confía. En la medida en que sus actos u omisiones causen daño a cualquiera de las demás, o contravengan sus obligaciones expresas o implícitas, cada una de ellas podrá ser tenida por responsable, o perder el derecho a invocar la responsabilidad, frente a otra parte. Se han adoptado varios enfoques legislativos de la responsabilidad en relación con la utilización de firmas digitales:

a) No establecer disposiciones expresas sobre normas de conducta o responsabilidad. Una opción podía ser que la ley guardara silencio sobre este aspecto. En los Estados Unidos de América, la ley sobre las firmas electrónicas en el comercio mundial y nacional (*Electronic Signatures in Global and National Commerce Act*) de 2000[217] no prevé la responsabilidad de ninguna de las partes que intervienen en el servicio de certificación. En términos generales, este criterio se ha adoptado en la

[216] Por ejemplo, el Grupo de trabajo sobre política de certificación del organismo federal de los Estados Unidos encargado de la política relativa a la infraestructura de clave pública elaboró una metodología para dictaminar sobre la equivalencia entre elementos de política (basada en el marco definido en RFC ("Request for Comments") 2527). Esta metodología puede utilizarse al evaluar distintas ICP o una de ellas con respecto a estas directrices (véase http://www.cio.gov/fpkipa, consultado el 6 de junio de 2008).

[217] Código de los Estados Unidos, título 15, capítulo 96, artículo 7031.

mayoría de los demás foros que adoptan un enfoque minimalista de la firma electrónica, como Australia[218];

b) Normas de conducta y régimen de responsabilidad aplicables únicamente al prestador de servicios de certificación. Otro enfoque es que en la norma legislativa se prevea únicamente la responsabilidad del prestador de servicios de certificación. Tal es el caso con arreglo a la Directiva 1999/93/CE de la Unión Europea por la que se establece un marco comunitario para la firma electrónica[219], en el párrafo 22 de cuyo preámbulo se establece que "los proveedores de servicios de certificación al público están sujetos a la normativa nacional en materia de responsabilidad", como se señala en el artículo 6 de la misma Directiva. Cabe observar que el artículo 6 se aplica únicamente a las "firmas reconocidas", lo que por ahora significa únicamente firmas digitales basadas en la infraestructura de clave pública[220];

c) Normas de conducta y régimen de responsabilidad para el firmante y el prestador de servicios de certificación. En algunos foros, la ley prevé la responsabilidad del firmante y del prestador de servicios de certificación, pero no establece ninguna norma en materia de diligencia para la parte que confía. Tal es el caso en China, con arreglo a la Ley sobre firma electrónica de 2005. La situación es semejante en Singapur, con arreglo a la Ley de operaciones electrónicas de 1998;

d) Normas de conducta y régimen de responsabilidad para todas las partes. Por último, la ley puede prever normas de conducta y establecer el fundamento del régimen de responsabilidad para todas las partes interesadas. Este criterio se adopta en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, en que se indican las obligaciones relativas al proceder del firmante (artículo 8), del prestador de servicios de certificación (artículo 9) y de la parte que confía en el certificado (artículo 11). Cabe afirmar que la Ley Modelo fija criterios para evaluar el proceder de esas partes. Sin embargo, deja en manos del derecho nacional determinar las consecuencias del incumplimiento de las diversas obligaciones y el fundamento del régimen de la responsabilidad de las diversas partes que utilicen sistemas de firma electrónica.

176. Las diferencias entre los regímenes de responsabilidad nacionales pueden obstaculizar el reconocimiento transfronterizo de las firmas electrónicas. Hay dos razones principales: En primer lugar, tal vez los prestadores de servicios de certificación no quieran reconocer certificados extranjeros o las claves expedidas por prestadores de servicios de certificación extranjeros cuya responsabilidad o cuyas normas en materia de diligencia sean menos estrictas que las suyas. En segundo, los usuarios de métodos

[218] Se consideró, por ejemplo, que los mecanismos de derecho privado admitidos en el ordenamiento jurídico de Australia, como las exclusiones contractuales, las cláusulas de renuncia y los descargos de responsabilidad, así como los límites a su aplicación impuestos por la *common law*, se prestaban mejor para reglamentar la responsabilidad que las disposiciones legislativas (véase Mark Sneddon, "*Legal liability and e-transactions — a Scoping Study for the National Electronic Authentication Council*", (National Office for the Information Economy, Canberra, 2000), págs. 43 a 47, que se puede consultar en http://unpan1.un.org/intradoc/groups/public/documents/ APCITY/UNPAN014676.pdf, (consultado el 6 de junio de 2008)).

[219] *Diario Oficial de las Comunidades Europeas*, L 13/12, 19 de enero de 2000.

[220] En la legislación aprobada en la Unión Europea se aplica este criterio, por ejemplo, en la Ley sobre firma electrónica de Alemania (SignaturGesetz, o SigG) y el reglamento correspondiente (SigV), de 2001, la Ley Federal sobre firma electrónica de Austria (SigG) y el Reglamento sobre firma electrónica del Reino Unido de Gran Bretaña e Irlanda del Norte, de 2002, artículo 4.

de firma y autenticación electrónicas, pueden temer que la imposición de una responsabilidad y una expectativa de diligencia menores al prestador de servicios de certificación extranjero limite los recursos con que puedan contar, por ejemplo, en caso de falsificación o defraudación. Por las mismas razones, en los casos en que la utilización de métodos de firma y autenticación electrónicas o las actividades de los prestadores de servicios de certificación se hallan previstas en la ley, ésta suele subordinar el reconocimiento de los certificados o los prestadores de servicios de certificación extranjeros a una evaluación de su equivalencia sustantiva con la fiabilidad de los certificados y los prestadores de servicios de certificación nacionales. El grado de diligencia y de responsabilidad que se espera de las diversas partes constituye la principal referencia jurídica para determinar esta equivalencia. Además, la capacidad del prestador de servicios de certificación de limitar su responsabilidad o exonerarse de ella repercutirá también en el grado de equivalencia que se atribuya a sus certificados.

1. Base de la responsabilidad en el marco de una infraestructura de clave pública

177. La asignación de responsabilidad en un marco de ICP se realiza en lo esencial de dos maneras: por medio de disposiciones contractuales o invocando normas de derecho (jurisprudencia, disposiciones legislativas o ambas). Las relaciones entre el prestador de servicios de certificación y el firmante son generalmente de tipo contractual, por lo que la responsabilidad se basa habitualmente en el incumplimiento de las obligaciones contractuales de cualquiera de las dos partes. Las relaciones entre el firmante y el tercero dependerán de la naturaleza de sus transacciones en cualquier caso determinado. Podrán o no basarse en un contrato. Por último, en la mayoría de los casos las relaciones entre el prestador de servicios de certificación y el tercero que confía no se basarían en un contrato[221]. En la mayoría de los ordenamientos jurídicos el fundamento de la responsabilidad (ya sea contractual o extracontractual) tendrá consecuencias amplias e importantes para el régimen de la responsabilidad, en particular por lo que atañe a los elementos siguientes: *a)* el grado de culpa necesario para invocar la responsabilidad de una parte (dicho de otra manera, el "grado de diligencia" que una parte debe a la otra); *b)* las partes que pueden reclamar indemnización por daños y la magnitud de aquéllos por los que puedan reclamarla; y *c)* si una parte culpable puede limitar su responsabilidad o exonerarse de ella y la medida en que pueda hacerlo.

178. Se desprende de lo anterior que el régimen de la responsabilidad varía no solo de un país a otro, sino también dentro de un mismo país, según la relación entre la parte a la que se tiene por responsable y la parte agraviada. Además, diversas normas y teorías jurídicas pueden repercutir en uno u otro aspecto de la responsabilidad en el marco de un régimen de responsabilidad basado en un contrato o en normas de

[221] Steffen Hindelang, en "No remedy for disappointed trust: the liability regime for certification authorities towards third parties outwith the EC Directive in England and Germany compared", *Journal of Information, Law and Technology*, Nº 1, 2002, disponible en http://www2.warwick.ac.uk/fac/ soc/law/elj/jilt/2002_1/hindelang, (consultado el 6 de junio de 2008), examina detalladamente la posibilidad de crear una relación contractual entre el prestador de servicios de certificación y un tercero conforme al derecho inglés, llegando a una conclusión negativa. Sin embargo, hay foros en que podría establecerse una relación contractual.

common law o del derecho legislativo, lo que en ocasiones reduce las diferencias entre los dos regímenes. El presente estudio no pretende realizar un análisis detallado y exhaustivo de estas cuestiones generales. En lugar de ello, se centra en las cuestiones que se plantean concretamente en un contexto de ICP, y examina brevemente la forma en que se han reglamentado en los respectivos ordenamientos jurídicos internos.

a) Grado de diligencia

179. Aunque en distintos ordenamientos jurídicos se utilizan diferentes sistemas y conceptos de clasificación, para los efectos del presente estudio se da por supuesto que en un marco de ICP la responsabilidad de las partes interesadas se basaría en lo esencial en tres criterios posibles: la negligencia o culpa simple; la presunta negligencia (o culpa con inversión de la carga de la prueba); y la responsabilidad objetiva[222].

i) *Negligencia simple*

180. Con arreglo a esta norma general, toda persona está legalmente obligada a indemnizar a otras por las consecuencias negativas de sus actos, siempre que la relación con esas personas presuponga en derecho la obligación de diligencia. Además, el grado de diligencia generalmente exigido es el de "diligencia razonable", que puede definirse sencillamente como el grado de diligencia con que procedería una persona dotada de sensatez, conocimientos y capacidad de previsión normales en las mismas circunstancias o en otras análogas. En los foros de derecho anglosajón, esto se suele denominar norma de razonabilidad ("reasonable person" standard), mientras que en varios foros de inspiración romanista se llama con frecuencia la norma del "buen padre de familia" ("bonus pater familias"). Desde la perspectiva estrictamente mercantil, por diligencia razonable se entiende el grado de diligencia con que procedería una persona de sensatez y capacidad normales que se dedicara al mismo tipo de actividad u oficio, en circunstancias semejantes. En los casos en que la responsabilidad se base en general en negligencia simple, corresponderá a la parte agraviada demostrar que el daño fue causado por el incumplimiento culposo de sus obligaciones por la otra parte.

181. La diligencia razonable (o la negligencia simple) es la norma general de diligencia prevista en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas. Esta norma en materia de diligencia se aplica a los prestadores de servicios de certificación con respecto a la expedición y revocación de certificados y la divulgación de información[223]. Pueden utilizarse varios elementos para evaluar el cumplimiento por los

[222] Con respecto al examen del régimen de responsabilidad en este contexto, véase Balboni, "Liability of certification service providers ...", págs. 232 y sigs.

[223] El párrafo 1 del artículo 9 de la Ley Modelo dispone lo siguiente: "Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios deberá": (...) "*b)* actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales; *c)* proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:" (...); "*d)* proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera: (...)".

prestadores de servicios de certificación de la norma general en materia de diligencia[224]. El mismo criterio se aplica a los firmantes respecto de la prevención del uso no autorizado y la protección de los dispositivos de creación de firmas[225]. La Ley Modelo aplica la misma norma general en materia de diligencia razonable a la parte que confía, que ha de adoptar medidas razonables para verificar tanto la fiabilidad de la firma electrónica como la validez, suspensión o revocación del certificado, y tener en cuenta cualquier limitación en relación con el certificado[226].

182. Unos pocos países, por lo general Estados promulgantes de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, han adoptado la norma general de "diligencia razonable" en lo tocante al proceder del prestador de servicios de certificación[227]. En algunos países, parece que el prestador de servicios de certificación ha de cumplir, con toda probabilidad, una norma general de diligencia razonable, aunque el hecho de que dicho prestador, por su naturaleza, sea una parte dotada de conocimientos especializados en que los legos confían más que en los agentes normales del mercado, podría, en último término, motivar que se le otorgara rango profesional o significar, por lo demás, que se le exigiera mayor diligencia en actuar de forma razonable en atención a sus aptitudes especializadas[228]. Ciertamente, como se expone más abajo (véase el párr. 29), tal parece ser el caso en la mayoría de los países.

183. Por lo que atañe al firmante, en algunos foros que han adoptado la Ley Modelo de la CNUDMI sobre Firmas Electrónicas se prevé una norma general de "diligencia razonable" [229]. En varios países la ley va acompañada de una lista más o menos extensa

---

[224] *Ley Modelo sobre Firmas Electrónicas...* El párrafo 146 de la Guía para la incorporación al derecho interno dispone que "Al evaluarse la responsabilidad del prestador de servicios de certificación, debían tenerse en cuenta, entre otras cosas, los siguientes factores: *a)* el costo de obtención del certificado; *b)* la naturaleza de la información que se certifique; *c)* la existencia de limitaciones de los fines para los que pueda utilizarse el certificado y el alcance de esas limitaciones; *d)* la existencia de declaraciones que limiten el alcance o la magnitud de la responsabilidad del prestador de servicios de certificación; y *e)* toda conducta de la parte que confía en la firma que contribuya a la responsabilidad. Durante la preparación de la Ley Modelo se convino en que, al determinar las pérdidas recuperables en el Estado promulgante, deberían tenerse en cuenta las normas que rijan la limitación de la responsabilidad en el Estado en que esté establecido el prestador de servicios de certificación o en cualquier otro Estado cuya legislación sea aplicable en virtud de las reglas pertinentes de conflicto de leyes".

[225] El artículo 8 de la Ley Modelo dispone lo siguiente: Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá: *a)* actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma; *b)* sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación, (...) o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si: i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;". Además, el firmante deberá "actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales".

[226] Apartado *a)* e incisos i) y ii) del apartado *b)* del artículo 11.

[227] Por ejemplo, las Islas Caimán, en su Ley de operaciones electrónicas de 2000, artículo 28, y Tailandia, en su Ley de operaciones electrónicas de 2001, artículo 28.

[228] "Certification authority: liability issues", preparado para la American Bankers Association por Thomas J. Smedinghoff, febrero de 1998, sección 1.1, disponible en http://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf, (consultado el 6 de junio de 2008).

[229] Por ejemplo, la Ley de operaciones electrónicas de Tailandia de 2001, artículo 27.

de obligaciones positivas, sin exponer el grado de diligencia previsto ni indicar las consecuencias del incumplimiento de esas obligaciones[230]. Sin embargo, en algunos países la ley complementa expresamente la lista de obligaciones con una declaración general de responsabilidad del firmante por su eventual incumplimiento[231], que en un caso es incluso de carácter penal[232]. Cabe afirmar que tal vez no haya una norma única en materia de diligencia sino un sistema escalonado con una norma general de diligencia razonable como regla supletoria con respecto a las obligaciones del firmante, que, sin embargo, pasa a ser una norma de garantía respecto de algunas obligaciones concretas, por lo general las relativas a la exactitud y veracidad de las declaraciones formuladas[233].

184. La situación de la parte que confía en el certificado es singular, porque resulta improbable que el firmante o el prestador de servicios de certificación resulten perjudicados por un acto u omisión de dicha parte que confía. En la mayoría de los casos, si la parte que confía no procede con el grado de diligencia necesario, sufriría las consecuencias de su proceder, pero no incurriría en responsabilidad respecto del prestador de servicios de certificación. Por ello, no es sorprendente que, al abordar la cuestión de las partes que confían, las distintas legislaciones nacionales relativas a la firma electrónica rara vez contengan más que una lista general de los deberes básicos de la parte que confía. Tal es el caso, por lo general, en los ordenamientos jurídicos que han aprobado la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, en que se recomienda una norma de "diligencia razonable" en relación con el proceder de la parte que

[230] Por ejemplo, la Argentina, Ley de firma digital de 2001, artículo 25; Chile, Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma de 2002, artículo 24; el Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, artículo 17; la India, Ley de la tecnología de la información de 2000, artículos 40 a 42; las Islas Caimán, Ley de operaciones electrónicas de 2000, artículo 31; Mauricio, Ley de operaciones electrónicas de 2000, artículos 33 a 36; el Perú, Ley de firmas y certificados digitales, artículo 17; Túnez, *Loi relative aux échanges et au commerce électroniques*, artículo 21; Turquía, Reglamento sobre los procedimientos y principios relativos a la aplicación de la Ley de firmas electrónicas de 2005, artículo 15; y Venezuela (República Bolivariana de), Ley sobre mensajes de datos y firmas electrónicas, artículo 19.

[231] China, Ley de firmas electrónicas, promulgada en 2004, artículo 27; Colombia, Ley 527 sobre comercio electrónico, artículo 40; México, Código de Comercio: Decreto sobre firma electrónica de 2003, artículo 99; República Dominicana, Ley sobre comercio electrónico, documentos y firmas digitales de 2002, artículos 53 y 55; Panamá, Ley de firma digital, 2001, artículos 37 y 39; Federación de Rusia, Ley federal sobre firmas electrónicas digitales de 2002, cláusula 12; Venezuela (República Bolivariana de), Ley sobre mensajes de datos y firmas electrónicas, artículo 19; y Viet Nam, Ley de operaciones electrónicas, artículo 25.

[232] Pakistán, Reglamento sobre las operaciones electrónicas de 2002, artículo 34.

[233] Por ejemplo, Singapur, Ley de operaciones electrónicas (capítulo 88). En el párrafo 2 del artículo 37 de esa Ley se dispone que al aceptar un certificado el firmante certifica ante todos quienes confían razonablemente en la información contenida en dicho certificado que: *a)* el suscriptor es el titular legítimo de la clave privada correspondiente a la clave pública señalada en el certificado; *b)* todas las declaraciones hechas por el suscriptor a la autoridad certificadora y que sirvan de fundamento a la información consignada en el certificado son veraces; y c) toda la información contenida en el certificado que se halle en conocimiento del suscriptor es veraz. A su vez, en el párrafo 1 del artículo 39 se prevé únicamente "la obligación de actuar con la debida diligencia para mantener el control de la clave privada que corresponda a la clave pública consignada en dicho certificado y prevenir su divulgación a toda persona no autorizada a crear la firma digital del suscriptor". Tal parece ser también el caso en la República Bolivariana de Venezuela, el artículo 19 de cuya Ley sobre mensajes de datos y firmas electrónicas condiciona expresamente la obligación de evitar el uso no autorizado del dispositivo de creación de la firma adscribiéndola a la necesidad de actuar con diligencia, mientras que otras obligaciones se establecen en términos categóricos.

confía[234]. Sin embargo, en algunos casos, este requisito no se indica expresamente[235]. Cabe señalar que las obligaciones expresas o implícitas de la parte que confía no son ajenas al prestador de servicios de certificación. Ciertamente, el incumplimiento por la parte que confía de su obligación de diligencia puede suministrar al prestador de servicios de certificación un argumento de defensa contra las reclamaciones de responsabilidad de la parte que confía, por ejemplo, cuando el prestador de servicios de certificación pueda demostrar que los perjuicios sufridos por la parte que confía podrían haberse evitado o mitigado si ésta hubiera adoptado medidas razonables para cerciorarse de la validez del certificado o los fines para los que podría utilizarse.

ii) *Presunción de negligencia*

185. La segunda posibilidad es un régimen basado en la culpa con inversión de la carga de la prueba. Con arreglo a este régimen, se presume la culpa de una parte cuando se hayan derivado perjuicios de un acto que se le pueda atribuir. El fundamento de este régimen es, por lo general, el supuesto de que, en determinadas circunstancias y en condiciones normales, los daños sólo pueden haberse producido porque una parte no ha cumplido sus obligaciones o no ha observado una norma de conducta que debía respetar.

186. En los ordenamientos de tradición romanista puede producirse una presunción de falta en relación con la responsabilidad por incumplimiento de contrato[236] y en algunos casos de responsabilidad extracontractual. Algunos ejemplos son la responsabilidad subsidiaria por los actos de empleados, agentes, niños o animales, y la responsabilidad surgida en el curso de alguna actividad comercial o industrial (daños ambientales, daños a propiedades adyacentes o accidentes de transporte). Las teorías que justifican la inversión de la carga de la prueba y los casos particulares en los que se admite varían en cada país.

187. En la práctica, ese sistema tiene un resultado similar al mayor grado de diligencia que se espera de los profesionales en el derecho anglosajón. Los profesionales deben tener un nivel mínimo de conocimientos y aptitudes especiales necesarios para

---

[234] Islas Caimán, Ley de operaciones electrónicas de 2000, artículo 21; México, Código de Comercio: Decreto sobre firma electrónica de 2003, artículo 107; y Tailandia, Ley de operaciones electrónicas de 2001, artículo 30.

[235] Turquía, Reglamento sobre los procedimientos y principios relativos a la aplicación de la Ley de firma electrónica de 2005, artículo 16; y Viet Nam, Ley de operaciones electrónicas, artículo 26.

[236] En el párrafo 1 del artículo 280 del Código Civil de Alemania, por ejemplo, se declara responsable del daño causado por el incumplimiento de una obligación contractual al deudor, a menos que éste no sea responsable del incumplimiento. En el párrafo 1 del artículo 97 del Código de Obligaciones de Suiza se consigna ese principio en términos todavía más claros: si el acreedor no obtiene la ejecución, el deudor deberá indemnizarlo por los daños resultantes, a menos que pueda demostrar que el incumplimiento de la ejecución no se debe a una falta suya. El artículo 1218 del Código Civil de Italia contiene una disposición similar. Según la legislación francesa, siempre se presume que ha habido negligencia si en el contrato se incluía la promesa de un resultado concreto, pero debe determinarse que ha habido negligencia si el objeto del contrato era ofrecer un nivel de ejecución, y no un resultado concreto (véase Gérard Légier, "Responsabilité contractuelle", *Répertoire de droit civil Dalloz*, Nº 58 a 68, agosto de 1989).

actuar como miembros de su profesión, y tienen la obligación de actuar como lo haría un miembro razonable de la profesión en cualquier circunstancia[237]. Ello no significa necesariamente que se invierta la carga de la prueba pero, en la práctica, el mayor grado de diligencia que se espera de los profesionales significa que se los considera capaces, si mantienen ese grado de diligencia, de evitar causar daños a las personas que contratan sus servicios o cuyo bienestar se les encomienda de otro modo. No obstante, en determinadas circunstancias el principio *res ipsa loquitur* permite a los tribunales suponer, a menos que se demuestre lo contrario, que sólo han podido producirse daños en el "curso ordinario de los acontecimientos" si una persona no ha actuado con diligencia razonable[238].

188. Si esa norma se aplica a las actividades de los prestadores de servicios de certificación, ello significaría que, si una parte que confía o un firmante sufren un perjuicio como resultado del uso de una firma electrónica o un certificado, y ese daño se puede atribuir al hecho de que el prestador de servicios de certificación no ha actuado de acuerdo con sus obligaciones contractuales o legales, entonces se presume que dicho prestador ha actuado con negligencia.

189. La presunción de negligencia parece ser el criterio preponderante en las legislaciones nacionales. Por ejemplo, en la directiva de la Unión Europea sobre la firma electrónica se establece que el prestador de servicios de certificación es responsable por el daño causado a cualquier entidad que confíe razonablemente en el certificado reconocido, salvo si prueba que no ha actuado con negligencia[239]. En otras palabras, la responsabilidad del prestador de servicios de certificación se basa en la negligencia, con una inversión de la carga de la prueba: el prestador debe demostrar que no actuó con negligencia, ya que es quien mejor puede demostrarlo por disponer de la pericia técnica y el acceso a la información pertinente necesarios (de los que posiblemente no dispongan ni el firmante ni los terceros que confían).

190. La misma situación se da en el marco de la legislación de diversos países no pertenecientes a la Unión Europea, que incluyen una larga lista de obligaciones que deben cumplir los prestadores de servicios de certificación y en los que, por lo general, se hace responsables de toda pérdida a los prestadores que no hayan cumplido sus

---

[237] W. Page Keeton y otros, "*Prosser and Keeton on the Law of Torts*", 5ª ed., (Saint Paul, Minnesota, West Publishing, 1984), sección 32, pág. 187.

[238] "Debe existir una prueba razonable de que se ha actuado con negligencia. Pero cuando se demuestra que el asunto está bajo control del demandado o de sus agentes, y el accidente es tal que en el curso ordinario de los acontecimientos no hubiera ocurrido si quienes tenían el control hubieran actuado con la debida diligencia, existirá una prueba razonable, en ausencia de una explicación por los demandados, de que el accidente se debió a una falta de diligencia." (C. J. Erle, en Scott v. *The London and St. Katherine's Docks Co*., Ex. Ch., 3 H & C 596, 601, 159 Eng. Rep. 665, 667 (1865)).

[239] *Diario Oficial de las Comunidades Europeas*, L 13/12, 19 de enero de 2001. En el artículo 6 de la Directiva se establece un grado mínimo de responsabilidad del prestador de servicios de certificación, que los Estados promulgantes podrían aumentar, por ejemplo, aplicando un régimen de responsabilidad objetiva o ampliando la responsabilidad a los certificados no reconocidos. Sin embargo, ello no ha ocurrido de momento y no es probable que ocurra, porque situaría a los prestadores de servicios de certificación de un país en desventaja frente a los de otros países de la Unión Europea (Balboni "Liability of certification service providers...", pág. 222).

obligaciones legales[240]. No está en absoluto claro si todos esos ordenamientos jurídicos invierten la carga de la prueba, pero algunos de ellos sí prevén explícitamente esa inversión, bien de manera general[241], o bien para obligaciones concretas[242].

191. Quizá se haya optado por un sistema de presunción de culpa porque se piense que la responsabilidad basada en la negligencia simple no sería justa para la parte que confía, pues tal vez ésta no disponga de los conocimientos tecnológicos ni del acceso a la información pertinente necesarios para demostrar que el prestador de servicios de certificación ha actuado con negligencia.

iii) *Responsabilidad objetiva*

192. La responsabilidad objetiva (*responsabilité objective*), o responsabilidad absoluta, es una norma que se utiliza en varios ordenamientos jurídicos para hacer responsable a una persona (generalmente, a fabricantes o explotadores de productos o equipos potencialmente peligrosos o nocivos) sin una constatación de culpa o de incumplimiento de la obligación de diligencia. Se considera que la persona es responsable simplemente por colocar en el mercado un producto defectuoso o por el mal funcionamiento de un aparato. Dado que se da por supuesta la responsabilidad por el mero hecho de haberse producido una pérdida o un daño, no hace falta determinar los elementos jurídicos necesarios para demostrar una acción como la negligencia, el incumplimiento de una garantía o la conducta intencional.

193. En la mayoría de ordenamientos jurídicos la responsabilidad objetiva es una norma excepcional que no se suele presumir, a menos que se indique claramente en un texto legislativo. En el contexto de los métodos de firma y autenticación electrónicas, la responsabilidad objetiva puede suponer una carga excesiva para el prestador de servicios de certificación, lo que a su vez quizá dificulte la viabilidad comercial de un sector que se encuentra en las primeras etapas de su desarrollo. De momento parece que ningún país impone una responsabilidad objetiva ni al prestador de servicios de certificación ni a ninguna de las demás partes

---

[240] Argentina, Ley de firma digital (2001), artículo 38; Chile, Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002), artículo 14; Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, artículo 31; Panamá, Ley de firma digital (2001), artículo 51, y Túnez, *Loi relative aux échanges et au commerce électroniques*, artículo 22.

[241] China, Ley de firmas electrónicas, promulgada en 2004, artículo 28: "Si un firmante electrónico o una persona que confía en una firma electrónica sufre una pérdida por confiar en el servicio de certificación de firma electrónica suministrado por un prestador de servicios de certificación electrónica en el curso de actividades civiles, ese prestador será responsable de los daños, salvo que demuestre que no ha cometido falta alguna"; véase también Turquía, Ley de firma electrónica de 2004, artículo 13: "Los prestadores de servicios de certificación electrónica estarán obligados a indemnizar por los daños sufridos por terceros como consecuencia de infracciones de las disposiciones de la presente ley o de los reglamentos promulgados en virtud de ella. Los prestadores de servicios de certificación electrónica quedarán exentos de esa obligación si demuestran que no ha habido negligencia."

[242] Barbados, capítulo 308B, Ley de operaciones electrónicas (1998), artículo 20: "Un prestador de servicios de certificación autorizado no será responsable de los errores de la información contenida en un certificado acreditado cuando: *a)* la información haya sido proporcionada por la persona identificada en el certificado acreditado o en su nombre; y *b)* el prestador de servicios de certificación pueda demostrar que ha adoptado todas las medidas razonablemente prácticas para verificar esa información."; véase también Bermudas, Ley de operaciones electrónicas (1999), apartado *b)* del párrafo 2 del artículo 23.

del proceso de la firma electrónica. Es cierto que en los países que exigen a los prestadores de servicios de certificación el cumplimiento de un gran número de obligaciones positivas, el grado de diligencia que se les pide suele ser muy alto, y en ocasiones es casi un régimen de responsabilidad objetiva, pero aun así, el prestador de servicios de certificación puede quedar exento de responsabilidad si demuestra que actuó con la diligencia debida[243].

b) Partes con derecho a reclamar daños y perjuicios y alcance de los daños y perjuicios exigibles

194. Una cuestión importante a la hora de determinar el grado de responsabilidad de los prestadores de servicios de certificación y los firmantes es la relativa al grupo de personas que pueden tener derecho a reclamar indemnización de los daños y perjuicios causados por el incumplimiento de cualquiera de las partes de sus obligaciones contractuales o legales. Otro asunto conexo es el alcance de la obligación de indemnizar y los tipos de daños y perjuicios por los que se debería indemnizar.

195. La responsabilidad contractual suele derivarse del incumplimiento de una obligación contractual. En un contexto de ICP generalmente existe un contrato entre el firmante y el prestador de servicios de certificación. Las consecuencias del incumplimiento de las obligaciones contractuales del uno frente al otro vienen determinadas por el texto del contrato, que se rige por el derecho de contratos aplicable. En el caso de las firmas y los certificados electrónicos, habría responsabilidad más allá de una relación contractual claramente definida, por ejemplo, cuando alguien ha sufrido un daño por confiar de manera razonable en la información proporcionada por el prestador de servicios de certificación o por el firmante, que ha resultado ser falsa o inexacta. El tercero que confía no suele celebrar un contrato con el prestador de servicios de certificación y probablemente no mantiene relación alguna con él excepto confiar en la certificación. Ello puede plantear cuestiones difíciles que algunos ordenamientos no han acabado de resolver.

196. En la mayoría de los ordenamientos jurídicos de tradición romanista se podría suponer que un prestador de servicios de certificación sería responsable de la pérdida sufrida por la parte que confía en el certificado como resultado de haber dado por buena información falsa o inexacta, incluso si la legislación sobre las firmas electrónicas aplicable no contiene disposiciones concretas al respecto. En algunos ordenamientos esa responsabilidad puede colegirse de la disposición general sobre responsabilidad extracontractual que se ha promulgado en la mayoría de ordenamientos de tradición romanista[244], con pocas excepciones[245]. En algunos ordenamientos podría establecerse

[243] Por ejemplo, en Chile, Ecuador y Panamá.

[244] En el artículo 1382 del Código Civil de Francia se establece que "cualquier" acto humano que cause daño a otra persona obliga a aquél por cuya culpa se produjo el daño a hacer efectiva una indemnización. Esta norma de responsabilidad general ha inspirado disposiciones parecidas en otros países, como el artículo 2043 del Código Civil de Italia y el artículo 483 del Código Civil de Portugal.

[245] El Código Civil de Alemania contiene tres disposiciones generales (artículos 823 I, 823 II y 826) y unas cuantas normas específicas que regulan una serie de situaciones enrevesadas definidas de manera bastante exhaustiva. La disposición principal es la contenida en el artículo 823 I, que difiere de la del Código Civil de Francia en que hace referencia expresa a los daños causados a "la vida, el cuerpo, la salud, la libertad, los bienes o cualquier otro derecho" de una persona.

una analogía entre las actividades de un prestador de servicios de certificación y los notarios, que suelen ser considerados responsables del daño causado por la negligencia cometida en el ejercicio de sus funciones.

197. En cambio, en los foros de derecho anglosajón la situación puede no estar tan clara. Si se ha cometido un hecho ilícito durante la ejecución de actos regidos por contrato, los foros de derecho anglosajón han requerido por lo general la existencia de algún tipo de relación contractual entre el autor del daño y la parte perjudicada. Dado que el tercero que confía no celebra un contrato con el prestador de servicios de certificación y probablemente no se relaciona con él en absoluto, excepto por el hecho de confiar en la certificación falsa, en algunos foros de derecho anglosajón puede resultar difícil que la parte que confía disponga de fundamentos para emprender actuaciones contra el prestador de servicios de certificación[246], a menos que exista una disposición legal explícita al respecto. Si no existe una relación contractual, para entablar una demanda por daños y perjuicios en el contexto de un ordenamiento de derecho anglosajón tendría que demostrarse que el autor del daño ha incumplido su deber de diligencia frente la parte perjudicada. No queda claro del todo si el prestador de servicios de certificación tiene dicho deber de diligencia frente todas las posibles partes que confían. En el derecho anglosajón suele haber reticencia a someter a alguien a una responsabilidad por falsedad negligente "de alcance indeterminado, por un período de tiempo indeterminado y ante un grupo indeterminado"[247], a menos que las palabras negligentes "se comuniquen directamente, con conocimiento o aviso de que se actuará en función de ellas, a alguien con quien el hablante está obligado a actuar con diligencia en todo momento porque existe una relación de deber surgida del ejercicio de un cargo público, de un contrato o por otro motivo"[248].

198. En ese caso la cuestión es determinar frente a qué grupo de personas un prestador de servicios de certificación (o incluso el firmante) es responsable de actuar con la debida diligencia. Básicamente, se pueden emplear tres criterios para definir el grupo de personas que en una situación de ese tipo pueden interponer con legitimidad una demanda contra el prestador de servicios de certificación[249]:

a) Criterio de previsibilidad. Es el criterio de responsabilidad más amplio. Según él, el firmante o el prestador de servicios de certificación son responsables ante toda persona que hubiera considerado razonablemente previsible confiar en las afirmaciones falsas;

---

[246] Por ejemplo, en el caso del derecho consuetudinario inglés, un autor concluye que "En ausencia de legislación, la responsabilidad [del prestador de servicios de certificación] ante [el tercero] no es en absoluto segura, aunque previsiblemente [el tercero] sufra una pérdida como resultado de su negligencia. Además, resulta difícil determinar cómo [el tercero] puede protegerse. Si no hay responsabilidad, al menos podría decirse que hay un vacío, y la negligencia del [prestador de servicios de certificación], en particular, crea un vacío claro. Quizá el derecho anglosajón solucione vacíos, pero el proceso es incierto y poco fiable" (Paul Todd, E-Commerce Law, (Abingdon, Oxon, Cavendish Publishing Limited, 2005), págs. 149 y 150). Se llegó a conclusiones similares respecto de la legislación australiana, véase Sneddon, "*Legal liability and e-transactions*...", pág. 15.

[247] Cita del juez Cardozo en el caso *Ultramares Corporation v. George A. Touche et al*, Tribunal de Apelación de Nueva York, 6 de enero de 1931, 174 N.E. 441, pág. 445.

[248] Cita del juez Cardozo en el caso *Ultramares Corporation v. George A. Touche et al*..., pág. 447.

[249] Smedinghoff, "Certification authority: liability issues"..., sección 4.3.1.

b) Criterio basado en el propósito y el conocimiento. Este criterio, más bajo, limita la responsabilidad a la pérdida sufrida por un integrante del grupo de personas para cuyo beneficio u orientación se pretende proporcionar información o se sabe que el destinatario pretende proporcionarla;

c) Criterio de la relación. Es el criterio más limitado. El deber existe únicamente frente al cliente o una persona con quien el proveedor de información tuviera contacto.

199. La Ley Modelo de la CNUDMI sobre Firmas Electrónicas no pretende delimitar el universo de personas que pueden incluirse en la categoría de "partes que confían en la firma"; podría tratarse de "cualquier persona, independientemente de si tiene una relación contractual con el firmante o con el prestador de servicios de certificación[250]". Del mismo modo, en la Directiva de la Unión Europea sobre la firma electrónica se establece que el prestador de servicios de certificación es responsable por el perjuicio causado "a cualquier entidad o persona física o jurídica que confíe razonablemente" en el certificado reconocido. Resulta claro que la Directiva de la Unión Europea se ha elaborado en torno a un plan de ICP, porque sólo es aplicable a las firmas digitales (certificados reconocidos). Por lo general se interpreta qué "entidad" se refiere a los terceros que confían, y la Directiva se ha aplicado en este sentido en todos los Estados de la Unión Europea, excepto en dos[251].

200 Al igual que la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, la Directiva de la Unión Europea sobre la firma electrónica tampoco limita las categorías de personas que pueden considerarse partes que confían. Por ello se ha sugerido que, incluso en los ordenamientos de derecho anglosajón, "en la prestación de servicios de certificación es evidente que un prestador de servicios de certificación está obligado a respetar el deber de diligencia frente a cualquier persona que pueda confiar en su certificado para decidir si acepta una firma electrónica concreta en una operación concreta, puesto que el propósito de expedir ese certificado es precisamente alentar a que se confíe en él[252]".

201. Otra cuestión de interés es la relativa a la naturaleza de los daños y perjuicios exigibles a un firmante o un prestador de servicios de certificación. Por ejemplo, en algunos foros de derecho anglosajón los daños y perjuicios puramente económicos causados por productos defectuosos no son exigibles en demandas civiles. Sin embargo, los casos de fraude intencional, o en algunos ordenamientos, incluso la falsedad negligente, se consideran excepciones a esa norma de la pérdida económica[253]. En relación con ello, es interesante comentar que el reglamento sobre firmas electrónicas del Reino Unido (2002) no reproduce las disposiciones relativas a la responsabilidad que aparecen en la Directiva de la Unión Europea sobre la firma electrónica. Por eso son aplicables las normas usuales de responsabilidad que, en este caso, están relacionadas

[250] *Ley Modelo de la CNUDMI sobre Firmas Electrónicas*..., párr. 150.

[251] Las excepciones son Dinamarca y Hungría (Balboni, "Liability of certification service providers ...", pág. 220.

[252] Lorna Brazell, "*Electronic Signatures: Law and Regulation*" (Londres, Sweet and Maxwell, 2004), pág. 187.

[253] Smedinghoff, "Certification authority: liability issues"..., sección 4.5.

con la prueba de la proximidad del daño[254]. La indemnización exigible suele dejarse en manos del derecho contractual o extracontractual general. Algunos ordenamientos obligan explícitamente a los prestadores de servicios de certificación a contratar seguros de responsabilidad civil o a informar a todos los posibles firmantes de las garantías económicas que cubren su posible responsabilidad, entre otras cosas[255].

c) Capacidad de limitar contractualmente la responsabilidad o renunciar a ella

202. Se supone que los prestadores de servicios de certificación tratan habitualmente de limitar en lo posible su responsabilidad contractual y extracontractual frente al firmante y las partes que confían. En cuanto al firmante, las cláusulas de limitación de responsabilidad suelen encontrarse en elementos de la documentación del contrato, como las declaraciones sobre prácticas de certificación (en las que se puede limitar la responsabilidad por incidente, por serie de incidentes o por período de tiempo, y se pueden excluir ciertos tipos de daños). Otra posibilidad consistiría en incluir en los certificados la cantidad máxima del valor de la operación para la que puede utilizarse el certificado, o limitar el uso del certificado a ciertos fines[256].

203. Si bien en la mayoría de regímenes jurídicos se reconoce el derecho de las partes contratantes a limitar o excluir la responsabilidad mediante disposiciones contractuales, ese derecho suele estar sujeto a varias limitaciones y condiciones. Por ejemplo, en la mayor parte de los ordenamientos de tradición romanista no se admite la exclusión total de la responsabilidad por la propia culpa de una persona[257], o se le imponen unas limitaciones claras[258]. Además, si los términos del contrato no se han negociado libremente sino que han sido impuestos o establecidos previamente por una de las partes (“contratos de adhesión”), algunos tipos de cláusulas de limitación pueden considerarse “abusivas” y, por tanto, nulas.

204. En los ordenamientos de derecho anglosajón se puede lograr un resultado similar a partir de varias teorías. Por ejemplo, en los Estados Unidos los tribunales no

---

[254] Dumortier y otros, “The legal and market aspects of electronic signatures”..., pág. 215.

[255] Turquía, Ley de firmas electrónicas (2004), artículo13; y Argentina, Ley de firma digital (2001), apartado *a)* del párrafo 1 del artículo 21; véase también México, Código de comercio: Decreto sobre firma electrónica (2003), artículo 104 III).

[256] Véase Smedinghoff, “Certification authority: liability issues”..., sección 5.2.5.4; y Hindelang, “No remedy for disappointed trust...”, sección 4.1.1.

[257] En Francia se puede excluir, en principio, la responsabilidad derivada del incumplimiento de contrato, pero en la práctica los tribunales suelen invalidar ese tipo de cláusulas siempre que se constate que eximirían a la parte de las consecuencias de un incumplimiento de una obligación contractual “fundamental” (véase Légier, “Responsabilité contractuelle”..., números 262 y 263).

[258] En la mayoría de países con ordenamientos de tradición romanista, la ley prohíbe el descargo de la responsabilidad derivada de negligencia grave o incumplimiento de una obligación impuesta por una norma de orden público. Algunos países cuentan con normas específicas a tal efecto, como el artículo 100 II del Código de Obligaciones de Suiza y el artículo 1229 del Código Civil de Italia. Otros países, como Portugal, no tienen una norma legal de ese tipo, pero obtienen prácticamente el mismo resultado que Italia (véase Antonio Pinto Monteiro, *Cláusulas Limitativas e de Exclusão de Responsabilidade Civil*, (Coimbra, Faculdade de Direito de Coimbra, 1985), pág. 217).

suelen hacer cumplir las disposiciones contractuales consideradas "leoninas". Aunque ese concepto normalmente depende de la determinación de las circunstancias particulares de cada caso, suele referirse a términos contractuales que "por una parte, nadie en su sano juicio establecería, a menos que se engañara, y, por otra parte, ninguna persona justa y honrada aceptaría[259]" y que se caracterizan porque "una de las partes no dispone de libertad real de elección y, además, los términos contractuales son excesivamente favorables a la otra parte[260]". De modo parecido a la noción de "contrato de adhesión" que se encuentra en los ordenamientos de tradición romanista, la doctrina se ha aplicado para evitar casos de "prácticas comerciales abusivas" por partes con un poder de negociación superior[261]. No todos los términos contractuales de ese tipo son nulos. Sin embargo, aunque los tribunales suelen hacer cumplir los contratos de modelo normalizado o de adhesión cuyos términos no son negociables, e incluso los contratos con consumidores, a veces un tribunal desestimará la ejecución de una cláusula de un contrato tipo si ello supone un resultado sorprendente e injusto[262].

205. Finalmente, tanto en los ordenamientos de tradición romanista como en los de derecho anglosajón, es posible que las normas de protección del consumidor reduzcan considerablemente la capacidad de un prestador de servicios de certificación de limitar su responsabilidad frente al firmante, en circunstancias en que esa limitación privaría al firmante de un derecho o recurso reconocidos por las leyes aplicables.

206. En la mayoría de casos la posibilidad de que el prestador de servicios de certificación limitara su responsabilidad potencial frente a la parte que confía estaría sujeta a restricciones aún mayores. A excepción de los modelos comerciales cerrados, en los que se exige a una parte que confía que cumpla los términos de un contrato[263], ocurre muy a menudo que la parte que confía no tiene obligaciones contractuales ante el prestador de servicios de certificación ni ante el firmante. Así, en la medida en que la parte que confía pueda tener derechos en el ámbito extracontractual frente al prestador de servicios de certificación o el firmante, quizá esas partes no tengan el modo de limitar su responsabilidad, porque en la mayoría de ordenamientos jurídicos ello requeriría informar debidamente de dicha limitación a la parte que confía. Dado que el prestador de servicios de certificación desconoce la identidad de la parte que confía antes de que se produzca el daño, tal vez no pueda aplicar un sistema eficaz de limitación de su responsabilidad (y posiblemente el firmante tenga todavía menos posibilidades de

[259] *First Financial Ins. Co. v. Purolator Security, Inc.*, 388 N.E.2d 17, 22 (Tribunal de Apelación del Primer Distrito de Illinois, 1979), citando a Hume v. U.S., 132 U.S. 406, 410 (1975), citado en Smedinghoff, "Certification authority: liability issues"..., sección 5.2.5.4.

[260] *First Financial Ins. Co. v. Purolator Security, Inc.* ..., citando a Williams v. Walker-Thomas Furniture Co., 350 F.2d 315, 320 (D.C. 1965), citado en Smedinghoff, "Certification authority: liability issues"..., sección 5.2.5.4.

[261] *First Financial Ins. Co. v. Purolator Security, Inc.*, 388 N.E.2d 17, 22 (Tribunal de Apelación del Primer Distrito de Illinois, 1979), citado en Smedinghoff, "Certification authority: liability issues"..., sección 5.2.5.4.

[262] Raymond T. Nimmer, *Information Law*, sección 11.12[4][a], págs. 11 a 37, citado en Smedinghoff, "Certification authority: liability issues"..., sección 5.2.5.4.

[263] Un ejemplo de esos modelos es el previsto para la E-Authentication Federation, entidad gestionada por la Administración de Servicios Generales del Gobierno de los Estados Unidos (véase E-Authentication Federation, Interim Legal Document Suite, versión 4.0.7, disponible en http://www.cio.gov/eauthentication/documents/LegalSuite.pdf, (consultado el 6 de junio de 2008)).

hacerlo). Es un problema típico de los sistemas abiertos en los que unos desconocidos interactúan sin contacto previo, que deja al firmante desprotegido ante consecuencias potencialmente devastadoras[264]. Muchos, en particular los representantes del sector de los servicios de certificación, consideraron esa situación un obstáculo importante al uso más extendido de los métodos de firma y autenticación electrónicos, dada la dificultad de los prestadores de servicios de certificación para evaluar su exposición a la responsabilidad.

207. Por deseo de aclarar ese punto jurídico, cierto número de países han reconocido expresamente el derecho de los prestadores de servicios de certificación de limitar su responsabilidad. Por ejemplo, la Directiva de la Unión Europea sobre la firma electrónica obliga a los Estados miembros de la Unión Europea a velar por que el prestador de servicios de certificación pueda consignar en un certificado reconocido "límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles para terceros[265]". Esos límites suelen ser de dos clases: límites a los tipos de operaciones para los que pueden usarse ciertos certificados o clases de certificados y límites al valor de las operaciones para las que se puede usar cierto certificado o clase de certificados. En los dos casos se dice expresamente que el prestador de servicios de certificación "no deberá responder de los daños y perjuicios causados por el uso de un certificado reconocido que exceda de los límites indicados en el mismo[266]". Además, la Directiva obliga a los Estados miembros de la Unión Europea a que velen por que el prestador de servicios de certificación "pueda consignar en un certificado reconocido un valor límite de las transacciones que puedan realizarse con el mismo, siempre y cuando los límites sean reconocibles para terceros[267]". En ese caso, el prestador de servicios de certificación no será responsable por los perjuicios que pudieran derivarse de la superación de ese límite máximo[268].

208. La Directiva de la Unión Europea sobre la firma electrónica no establece un tope de la responsabilidad en la que puede incurrir un prestador de servicios de certificación, pero le permite indicar el valor máximo por operación que se realice con los certificados, con lo cual lo exime de la responsabilidad que supere ese tope del valor[269]. A modo de práctica comercial, los prestadores de servicios de certificación a menudo introducen también con carácter contractual un tope global de su responsabilidad en los contratos.

209. En otros ordenamientos jurídicos nacionales se apoyan esas prácticas contractuales admitiendo un límite a la responsabilidad de los prestadores de servicios de certificación frente a cualquier parte potencialmente afectada. Por lo general esas leyes

---

[264] Sneddon, "*Legal liability and e-transactions* ...", pág. 18.

[265] Directiva de la Unión Europea sobre la firma electrónica, artículo 6, párrafo 3.

[266] Directiva de la Unión Europea sobre la firma electrónica...

[267] Directiva de la Unión Europea sobre la firma electrónica, artículo 6, párrafo 4.

[268] Directiva de la Unión Europea sobre la firma electrónica...

[269] Dumortier y otros, "The legal and market aspects of electronic signatures"..., pág. 55; véase también Hindelang, "No remedy for disappointed trust ...", sección 4.1.1.; Balboni ("Liability of certification service providers ...", pág. 230) va más allá y dice que "según el párrafo 4 del artículo 6, sólo es posible establecer un límite al valor de la operación [...], lo que no guarda relación alguna con una limitación de la cantidad potencial de daño que pueda derivarse de esa operación".

permiten establecer las limitaciones que se especifiquen en la declaración de prácticas de certificación del prestador de servicios de certificación, y en algunos casos lo eximen expresamente de la responsabilidad si un certificado se utiliza para un fin distinto a aquél para el que se expidió[270]. Además, algunos ordenamientos reconocen el derecho de los prestadores de servicios de certificación de expedir certificados de diferentes clases y de establecer diferentes niveles de confianza recomendados[271], a los que suelen corresponderse diferentes niveles de limitación (y de seguridad), según la tasa pagada. No obstante, algunas normativas prohíben expresamente toda limitación de la responsabilidad, excepto la que resulta de limitar la utilización o el valor de los certificados[272].

210. Los países que han adoptado un enfoque minimalista también han considerado que por lo general no era aconsejable la intervención legislativa, y han preferido dejar que las partes regulen la cuestión por contrato[273].

2. Casos especiales de responsabilidad en el marco de una infraestructura de clave pública

211. Las deliberaciones sobre la responsabilidad generada por la utilización de métodos de autenticación y firma electrónicas se han centrado principalmente en el fundamento y las características de la responsabilidad de los prestadores de servicios de certificación. En general se acepta que la obligación básica de éstos es utilizar sistemas, procedimientos y recursos humanos fiables y actuar de conformidad con las declaraciones que hagan respecto de sus normas y prácticas[274]. También se supone que han de actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que hayan hecho en relación con un certificado sean exactas y cabales. Todas esas actividades pueden generarles diversos grados de responsabilidad, según el derecho aplicable. En los párrafos siguientes se mencionan casos en que los prestadores de servicios de certificación corren más riesgo de incurrir en responsabilidad y se reseñan las formas en que se aborda esa cuestión en diversos ordenamientos jurídicos.

---

[270] Argentina, Ley de firma digital (2001), artículo 39; Barbados, capítulo 308B, Ley de operaciones electrónicas (1998), artículo 20, párrafos 3 y 4; Bermudas, Ley de operaciones electrónicas (1999), artículo 23, párrafos 3 y 4; Chile, Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002), artículo 14; y Viet Nam, Ley de operaciones electrónicas, artículo 29, párrafos 7 y 8 (esta última no hace mención expresa a la exención de responsabilidad).

[271] Singapur, Ley de operaciones electrónicas (capítulo 88) (1988), artículos 44 y 45; y Mauricio, Ley de operaciones electrónicas (2000), artículos 38 y 39.

[272] Turquía, Ley de firmas electrónicas (2004), artículo 13.

[273] En el caso de Australia, véase Sneddon, "Legal liability and e-transactions...", págs. 44 a 47; en cuanto a los Estados Unidos, véase Smedinghoff, "Certification authority: liability issues"..., sección 5.2.51.

[274] Ley Modelo de la CNUDMI sobre Firmas Electrónicas..., apartados *a)* y *b)* del párrafo 1 del artículo 9.

a) Cuando no se expide un certificado o se demora en expedirlo

212. El prestador de servicios de certificación normalmente expide certificados en respuesta a solicitudes de posibles firmantes. Si la solicitud cumple los criterios establecidos por el prestador de servicios de certificación, éste puede extender el certificado. Es posible que un solicitante cumpla esos criterios y de todas formas su solicitud sea rechazada o aplazada, ya sea porque el prestador de servicios comete un error, porque los medios que utiliza para atender a las solicitudes han quedado fuera de servicio, involuntaria o deliberadamente, o porque por otros motivos desea retrasar o denegar la expedición del certificado. En esas circunstancias, el solicitante cuya solicitud sea rechazada o demorada tal vez pueda demandar al prestador de servicios de certificación[275].

213. Si existe un mercado competitivo de servicios de certificación, en realidad el solicitante puede no resultar perjudicado cuando un prestador de servicios de certificación se niegue a extenderle el certificado, involuntaria o deliberadamente. Sin embargo, si no existe una competencia real, el hecho de que el prestador de servicios de certificación se niegue a extender el certificado o retrase su expedición podría causar graves perjuicios si el solicitante rechazado no pudiera llevar a cabo determinado negocio sin el certificado. Aun cuando existieran opciones competitivas, podría considerarse que el hecho de retrasar o denegar la expedición de un certificado solicitado en relación con una operación determinada redundaría en perjuicio del solicitante si éste tuviese que renunciar a una operación valiosa por no disponer de él a tiempo[276].

214. Es improbable que se plantee esa clase de hipótesis en un contexto internacional, ya que la mayoría de los firmantes muy probablemente recurrirían a prestadores de servicios de certificación situados en sus propios países.

b) Cuando se actúa con negligencia al extender un certificado

215. La función principal de un certificado es vincular la identidad del firmante a una clave pública. En consecuencia, la tarea principal del prestador de servicios de certificación es verificar, de conformidad con sus prácticas establecidas, que el solicitante sea el presunto firmante y ejerza el control de la clave privada correspondiente a la clave pública indicada en el certificado. Si no lo hace, puede incurrir en responsabilidad frente al firmante o frente a un tercero que confíe en el certificado.

216. El firmante podría sufrir perjuicios, por ejemplo, si se hubiera expedido erróneamente un certificado a un impostor que hubiera usurpado su identidad. Los propios empleados o contratistas del prestador de servicios de certificación podrían confabularse para expedir certificados erróneos utilizando la clave de firma de éste para atender a solicitudes indebidas del impostor. Esas personas podrían actuar con negligencia y expedir un certificado erróneo, ya sea aplicando indebidamente los procedimientos

[275] Smedinghoff "Certification authority: liability issues"..., sección 3.2.1.

[276] Smedinghoff "Certification authority: liability issues"..., sección 3.2.1.

de validación establecidos por el prestador de servicios de certificación al examinar la solicitud del impostor o utilizando la clave de firma del prestador de servicios de certificación para crear un certificado que no ha sido aprobado. Por último, un malhechor podría hacerse pasar por el firmante utilizando documentos de identificación falsificados, aunque aparentemente auténticos, y convencer al prestador de servicios de certificación, aun cuando éste se adhiera cuidadosamente a sus normas establecidas y no actúe con negligencia, a extenderle un certificado[277].

217. El hecho de extender un certificado erróneo a un impostor podría tener consecuencias muy graves. Las partes que confían y que realicen operaciones en línea con el impostor pueden confiar en los datos incorrectos del certificado expedido erróneamente y, por consiguiente, despachar mercancías, transferir fondos, conceder crédito o llevar a cabo otras operaciones en la creencia de que está tratando con la persona cuya identidad ha sido suplantada. Cuando se descubra el fraude, las partes que hayan confiado en el certificado pueden haber sufrido grandes pérdidas. En este caso hay dos partes perjudicadas: la que confió en el certificado expedido erróneamente y fue víctima de fraude y la persona cuya identidad fue suplantada en el certificado expedido erróneamente. Ambas podrán demandar al prestador de servicios de certificación. Otra hipótesis podría ser la negligencia al extender un certificado a una persona imaginaria, en cuyo caso sólo resultarían perjudicadas las partes que confiaran en él[278].

218. El artículo 9 de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas dispone, entre otras cosas, que el prestador de servicios de certificación actúe "con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales". Esta obligación general se ha trasladado literalmente a la legislación de varios países que aplican la Ley Modelo[279], si bien en algunos países la norma parece haberse hecho más estricta y, en lugar de "diligencia razonable", se exigen mayores garantías[280].

219. El régimen establecido por la Directiva de la Unión Europea sobre la firma electrónica obliga a los Estados miembros de la Unión Europea a garantizar, "como mínimo", que el prestador de servicios de certificación que expida al público un certificado presentado como certificado reconocido o que garantice al público tal certificado sea responsable del perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en el certificado por lo que respecta a: *a)* la veracidad, en el momento de su expedición, de toda la información contenida en el certificado reconocido y la inclusión en el certificado de toda la información prescrita para los certificados reconocidos; *b)* la garantía de que, en el momento de la expedición del

[277] Smedinghoff "Certification authority: liability issues"..., sección 3.2.1.

[278] Smedinghoff "Certification authority: liability issues"..., sección 3.2.1.

[279] Por ejemplo, Tailandia, Ley de operaciones electrónicas (2001), artículo 28, párrafo 2; e Islas Caimán (territorio de ultramar del Reino Unido), Ley de operaciones electrónicas, 2000, artículo 28 *b)*.

[280] Por ejemplo, China, Ley sobre las firmas electrónicas, artículo 22: "Los prestadores de servicios de certificación electrónica deberán garantizar que el contenido de los certificados de firmas electrónicas sea cabal y exacto durante su plazo de validez y que las partes que confíen en las firmas electrónicas puedan verificar o comprender la totalidad del contenido registrado de los certificados de firmas electrónicas y las demás cuestiones pertinentes", sin negrita en el original.

certificado, obraban en poder del firmante identificado en el certificado reconocido los datos de creación de firma correspondientes a los datos de verificación de firma que constan o se identifican en el certificado; *c)* la garantía de que los datos de creación y de verificación de firma pueden utilizarse complementariamente, en caso de que el prestador de servicios de certificación genere ambos; salvo que el prestador de servicios de certificación demuestre que no ha actuado con negligencia[281].

220. Otros ordenamientos jurídicos nacionales suelen coincidir en imponer a los prestadores de servicios de certificación la obligación de verificar la exactitud de la información en que se basan para extender un certificado. En algunos países el prestador de servicios de certificación suele ser considerado responsable frente a toda persona que confíe razonablemente en el certificado de la exactitud de toda la información que conste en el certificado acreditado en la fecha en que fue expedido[282], o garantiza su exactitud[283], si bien en algunos de esos países puede condicionar esa garantía formulando la declaración correspondiente en el certificado[284]. No obstante, algunas leyes lo exoneran expresamente de responsabilidad con respecto a la inexactitud de la información facilitada por el firmante que, conforme a lo dispuesto en la declaración sobre las prácticas de certificación, deba ser objeto de verificación, siempre y cuando el prestador de servicios de certificación pueda demostrar que ha tomado "todas las medidas razonables" para verificar la información[285].

221. En otros países se obtiene el mismo resultado no mediante una garantía prevista en la ley, sino imponiendo a los prestadores de servicios de certificación el deber general de verificar la información facilitada por el firmante antes de extender un certificado[286] o de mantener sistemas de respaldo de la información relativa a los certificados[287]. En algunos casos el prestador de servicios de certificación está obligado a revocar un certificado inmediatamente después de que determine que la información en que se basó para expedirlo era inexacta o falsa[288]. Sin embargo, en unos pocos casos la ley guarda silencio con respecto a la expedición de certificados y simplemente exige que el prestador de servicios de certificación dé cumplimiento a su declaración de prácticas de certificación[289] o expida el certificado conforme a lo

---

[281] Directiva de la Unión Europea sobre la firma electrónica..., artículo 6, párrafo 1.

[282] Barbados, capítulo 308B, Ley de operaciones electrónicas (1998), artículo 20, párrafo 1) *a)*; Bermudas, Ley de operaciones electrónicas, 1999, artículo 23; Región Administrativa Especial de Hong Kong de China, Ordenanza sobre operaciones electrónicas, artículo 39; India, Ley sobre tecnología de la información, 2000, artículo 36 *e)*; Mauricio, Ley sobre operaciones electrónicas, 2000, artículo 27, párrafo 2) *d)*, y Singapur, Ley de operaciones electrónicas, artículo 29 2) *a)* y *c)* y artículo 30, párrafo 1).

[283] Túnez, *Loi relative aux échanges et au commerce électronique*, artículo 18 ; y Viet Nam, Ley de operaciones electrónicas, artículo 31 *d)*.

[284] Por ejemplo, en Barbados, Bermudas, RAE de Hong Kong de China, Mauricio y Singapur.

[285] Argentina, Ley de firma digital (2001), artículo 39 *c)*.

[286] Argentina, Ley de firma digital (2001), artículo 21 *o)*; Chile, Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, artículo 12 *e)*; México, Código de Comercio: Decreto sobre Firma Electrónica (2003), artículo 104 I); y Venezuela (República Bolivariana de), Ley sobre mensajes de datos y firmas electrónicas", artículo 35.

[287] Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, artículo 30 *d)*.

[288] Argentina, Ley de firma digital (2001), artículo 19 *e)* 2).

[289] Perú, Decreto reglamentario de la ley de firmas y certificados digitales, artículo 29 *a)*.

acordado con el suscriptor[290]. Esto no significa que la ley no prevea responsabilidad alguna de los prestadores de servicios de certificación. Por el contrario, en algunas leyes se determina claramente la responsabilidad de éstos al exigirles que contraten un seguro adecuado de responsabilidad civil que cubra todos los perjuicios contractuales y extracontractuales de los signatarios y terceros de buena fe[291].

222. El deber del prestador de servicios de certificación de verificar la exactitud de la información proporcionada se complementa con el deber del firmante de "actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales" [292]. En consecuencia, el firmante podría incurrir en responsabilidad, ya sea frente al prestador de servicios de certificación o frente a la parte que confíe en el certificado, por proporcionar información falsa o inexacta al prestador de servicios de certificación en el momento de solicitarlo. Algunas veces esto se formula imponiendo el deber general de proporcionar información exacta al prestador de servicios de certificación[293] o de actuar con diligencia razonable para garantizar la veracidad de la información[294], y otras veces se declara al firmante expresamente responsable de los daños provocados por el incumplimiento de este deber[295].

c) Uso de la firma sin autorización o validez cuestionable de la firma

223. El uso sin autorización de dispositivos de creación de firma y de certificados reviste dos aspectos. Por una parte, es posible que el dispositivo de creación de firma no esté debidamente protegido o que su seguridad se vea comprometida de otra manera, por ejemplo, por apropiación indebida perpetrada por un agente del firmante. En cambio, la jerarquía del propio prestador de servicios de certificación con respecto a la firma puede quedar en entredicho, por ejemplo, si su clave de firma o la clave básica se pierde, se divulga o es utilizada por otras personas sin autorización, o si se ve comprometida de alguna otra manera.

224. La jerarquía con respecto a la firma puede quedar en entredicho de varias formas. El prestador de servicios de certificación o uno de sus empleados o contratistas puede destruir accidentalmente la clave o perder el control de ésta; el centro de datos de la clave privada puede sufrir daños de resultas de un accidente, o la clave del prestador de servicios de certificación puede ser destruida deliberadamente o puede ser invalidada con

---

[290] Colombia, Ley 527 sobre comercio electrónico, artículo 32 *a)*; Panamá, Ley de firma digital (2001), artículo 49, párrafo 7); y República Dominicana, Ley sobre comercio electrónico, documentos y firmas digitales (2002), artículo 40 *a)*.

[291] República Bolivariana de Venezuela, Ley sobre mensajes de datos y firmas electrónicas, artículo 32.

[292] Ley Modelo de la CNUDMI sobre Firmas Electrónicas..., artículo 8, apartado *c)* del párrafo 1.

[293] Argentina, Ley de firma digital (2001), artículo 25; Chile, Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002), artículo 24; y México, Código de Comercio: Decreto sobre firma electrónica (2003), artículo 99 III).

[294] Islas Caimán, Ley de operaciones electrónicas de 2000, artículo 31 *c)*.

[295] Colombia, Ley 527 sobre comercio electrónico, artículo 40; México, Código de Comercio: Decreto sobre firma electrónica (2003), artículo 99 III); Panamá, Ley de firma digital (2001), artículo 39; y República Dominicana, Ley sobre comercio electrónico, documentos y firmas digitales (2002), artículo 55.

fines ilícitos (por ejemplo, por un pirata informático). Las consecuencias de que la jerarquía con respecto a la firma quede comprometida podrían ser muy graves. Por ejemplo, si la clave privada o las claves básicas cayeran en manos de un malhechor, éste podría generar certificados falsos y utilizarlos para suplantar la identidad de firmantes reales o imaginarios en detrimento de las partes que confíen en los certificados. Por otra parte, una vez que el hecho se descubriera, habría que revocar todos los certificados expedidos por ese prestador de servicios de certificación, lo que daría lugar a posibles demandas en masa de todos los firmantes por inutilización de sus firmas.

225. Esta cuestión no se aborda en detalle en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas. Cabe presumir que la obligación general del prestador de servicios de certificación prevista en la Ley Modelo, en cuanto a "utilizar sistemas, procedimientos y recursos humanos fiables"[296], abarca el deber de adoptar todas las medidas que sean necesarias para impedir que su propia clave (y, por lo tanto, su jerarquía con respecto a la firma) quede en entredicho. Las leyes de varios países disponen expresamente esa obligación, con frecuencia combinada con la de utilizar sistemas fiables[297]. En algunos casos existe el deber específico de adoptar medidas para evitar la falsificación de certificados[298]. El prestador de servicios de certificación debe abstenerse de generar datos de creación de firma de los titulares de certificados o de acceder a esos datos y puede tener que responder de los actos de sus empleados que deliberadamente lo hayan hecho[299]. El prestador de servicios de certificación tendría la obligación de solicitar la revocación de su propio certificado si los datos de creación de la firma quedaran comprometidos[300].

226. El firmante también debe actuar con la debida diligencia. Por ejemplo, en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas se exige al firmante que "actúe con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma"[301]. En la mayoría de los ordenamientos jurídicos se impone una obligación análoga, si bien con algunas variaciones. En algunos casos la ley impone al firmante la obligación estricta de ejercer control exclusivo sobre el dispositivo de creación de firma e impedir que se utilice sin autorización[302], o declara al firmante único responsable de salvaguardar el dispositivo de creación de firma[303]. No obstante, esa obligación suele estar calificada como deber de ejercer control adecuado sobre el dispositivo de

---

[296] Artículo 9, párrafo 1 *f)*.

[297] Argentina, Ley de firma digital (2001), artículo 21 *c)* y *d)*; Colombia, Ley 527 sobre comercio electrónico, artículo 32 b); Mauricio, Ley de operaciones electrónicas 2000, artículo 24; Panamá, Ley de firma digital (2001), artículo 49, párrafo 5; Tailandia, Ley de operaciones electrónicas (2001), artículo 28, párrafo 6, y Túnez, *Loi relative aux échanges et au commerce électroniques*, artículo 13.

[298] República Bolivariana de Venezuela, Ley sobre mensajes de datos y firmas electrónicas, artículo 35.

[299] Argentina, Ley de firma digital (2001), artículo 21 *b)*.

[300] Argentina, Ley de firma digital (2001), artículo 21 *p)*.

[301] Artículo 8, párrafo 1 *a)*.

[302] Argentina, Ley de firma digital (2001), artículo 25 *a)*; Colombia, Ley 527 sobre comercio electrónico, artículo 39, párrafo 3; Federación de Rusia, Ley Federal sobre la firma digital electrónica (2002), cláusula 12, párrafo 1; Panamá, Ley de firma digital (2001), artículo 37, párrafo 4; República Dominicana, Ley sobre comercio electrónico, documentos y firmas digitales (2002), artículo 53 *d)*; y Turquía, Ordenanza sobre los procedimientos y principios relativos a la aplicación de la Ley de la firma electrónica (2005), artículo 15 *e)*.

[303] Túnez, *Loi relative aux échanges et au commerce électroniques*, artículo 21.

creación de firma o de adoptar medidas adecuadas para ejercer control sobre éste[304], de actuar con diligencia para evitar el uso no autorizado[305], o de actuar con diligencia razonable para evitar que el dispositivo de firma se utilice sin autorización[306].

d) El hecho de no suspender o no revocar un certificado

227. El prestador de servicios de certificación también podría incurrir en responsabilidad por no suspender o no revocar un certificado de validez cuestionable. Para que una infraestructura de firmas digitales funcione correctamente e inspire confianza, es esencial contar con un mecanismo para determinar en tiempo real si determinado certificado es válido o si se ha suspendido o revocado. Por ejemplo, cuando una clave privada haya quedado comprometida, la revocación del certificado es el principal mecanismo por el cual el firmante puede protegerse de operaciones fraudulentas iniciadas por impostores que pueden haber obtenido una copia de la clave.

228. En consecuencia, la rapidez con que el prestador de servicios de certificación revoque o suspenda el certificado del firmante tras haber recibido la solicitud de éste es crítica. Si transcurre cierto período entre la solicitud del firmante de que se revoque el certificado, la revocación efectiva y la publicación del aviso de revocación, un impostor tendría la posibilidad de iniciar operaciones fraudulentas. Así pues, si el prestador de servicios de certificación no inscribe la revocación de un certificado en la lista de certificados revocados o retrasa irrazonablemente la inscripción, tanto el firmante como la parte que confió en el certificado y fue víctima de fraude podrían sufrir perjuicios considerables por fiarse de un certificado presuntamente válido. Además, como parte de sus servicios de certificación, los prestadores pueden ofrecer repertorios y listas de certificados revocados a que puedan acceder electrónicamente los interesados. Llevar esa base de datos esencialmente entraña dos riesgos: que el repertorio o lista de certificados revocados contenga errores y, por lo tanto, proporcione información inexacta en detrimento de la persona que lo reciba y confíe en él, y que no se pueda acceder al repertorio o lista de certificados revocados (por ejemplo, por un fallo del sistema), lo que socavará la capacidad de los firmantes y de las partes que confíen en el certificado para llevar a feliz término las operaciones.

229. Como se indicó anteriormente, en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas se presume que el prestador de servicios de certificación podrá expedir certificados de diversos niveles y grados de fiabilidad y seguridad. Por consiguiente, la Ley Modelo no exige que el prestador de servicios de certificación siempre ofrezca un sistema de revocación, lo que puede no ser rentable cuando se trate de ciertos

[304] Chile, Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002), artículo 24; y Viet Nam, Ley de operaciones electrónicas, artículo 25, párrafo 2 *a)*.

[305] República Bolivariana de Venezuela, Ley sobre mensajes de datos y firmas electrónicas, artículo 19.

[306] Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, artículo 17 *b)*; India, Ley 21 de tecnología de la información, 2000, artículo 42 1); Islas Caimán, Ley de Operaciones Electrónicas, 2000, artículo 39 a); Mauricio, Ley de operaciones electrónicas de 2000 artículo 35, párrafo 1 *a)* y *b)*; México, Código de Comercio: Decreto sobre firma electrónica (2003), artículo 99 II); Singapur, Ley de operaciones electrónicas, capítulo 88, artículo 39, y Tailandia, Ley de operaciones electrónicas (2001), artículo 27, párrafo 1.

tipos de certificados de escaso valor. En cambio, la Ley Modelo únicamente exige que el prestador de servicios de certificación proporcione a la parte que confía en el certificado "medios razonablemente accesibles" que le permitan determinar mediante el certificado, entre otras cosas, "si existe un medio para que el firmante dé aviso" de que los datos de creación de la firma están en entredicho y "si se ofrece un servicio para revocar oportunamente el certificado"[307]. Si se ofrece ese servicio, el prestador de servicios de certificación está obligado a cerciorarse de que ese servicio exista[308].

230. El régimen establecido por la Directiva de la Unión Europea sobre la firma electrónica obliga a los Estados miembros de la Unión Europea a garantizar, "como mínimo", que el prestador de servicios de certificación que haya expedido al público un certificado presentado como certificado reconocido sea responsable por el perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en dicho certificado por no haber registrado la revocación del certificado, salvo que el prestador de servicios de certificación pruebe que no ha actuado con negligencia[309]. En algunas legislaciones nacionales se obliga al prestador de servicios de certificación a adoptar medidas para impedir la falsificación de certificados[310] o a revocar el certificado inmediatamente después de que se determine que estaba basado en información inexacta o falsa[311].

231. También puede imponerse una obligación análoga al firmante y a otras personas autorizadas. Por ejemplo, en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas se dispone que el firmante "sin dilación indebida" utilice "los medios que le proporcione el prestador de servicios de certificación", o "en cualquier caso se esfuerce razonablemente para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen", si el firmante "sabe que los datos de creación de la firma han quedado en entredicho" o si "las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho"[312].

232. En las leyes de algunos países con frecuencia se afirma el deber del firmante de solicitar la revocación de su certificado ante cualquier circunstancia que pueda haber puesto en entredicho el carácter secreto de sus datos de creación de firma[313], si bien en algunos casos la ley únicamente obliga al firmante a comunicar ese hecho al prestador

---

[307] Artículo 9, párrafo 1 *d)*, v) y vi).

[308] Artículo 9, párrafo 1 *e)*.

[309] Directiva de la Unión Europea sobre la firma electrónica..., artículo 6 , párrafo 2; véase también el apartado *b)* del anexo II de la Directiva.

[310] Panamá, Ley de firma digital (2001), artículo 49, párrafo 6.

[311] Argentina, Ley de firma digital (2001), artículo 19 *e)* 2).

[312] Artículo 8, párrafo 1 *b)*, i) y ii).

[313] Argentina, Ley de firma digital (2001), artículo 25 *c)*; Colombia, Ley 527 sobre comercio electrónico, artículo 39, párrafo 4; Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, artículo 17 *f)*; Federación de Rusia, Ley Federal sobre las firmas digitales electrónicas (2002), cláusula 12, párrafo 1; Mauricio, Ley de operaciones electrónicas, (2000), artículo 36; Panamá, Ley de firma digital (2001), artículo 37, párrafo 5; República Dominicana, Ley sobre comercio electrónico, documentos y firmas digitales (2002), artículos 49 y 53 *e)*; y Singapur, Ley de operaciones electrónicas (capítulo 88), artículo 40.

de servicios de certificación[314]. Las leyes de varios países han adoptado la formulación de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, que impone al firmante la obligación de dar aviso, además, a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen[315]. Si bien en algunos ordenamientos jurídicos las consecuencias del incumplimiento de ese deber pueden estar implícitas, en algunos países la ley declara expresamente al firmante responsable si no da oportuno aviso de la pérdida del control de la clave privada o si no solicita la revocación del certificado[316].

Conclusión

233. El empleo generalizado de métodos de autenticación y firma electrónicas puede constituir un medio importante para reducir la documentación comercial y los costos que entraña en las operaciones internacionales. Si bien el ritmo de avance en esta esfera está determinado en gran medida principalmente por la calidad y la seguridad de las soluciones tecnológicas, las normas jurídicas pueden coadyuvar considerablemente a facilitar el empleo de los métodos de autenticación y firma electrónicas.

234. Muchos países ya han adoptado medidas a nivel interno en ese sentido promulgando leyes que afirman el valor jurídico de las comunicaciones electrónicas y determinan los criterios necesarios para establecer su equivalencia con las comunicaciones consignadas sobre papel. Las disposiciones que rigen los métodos de autenticación y firma electrónicas suelen ser un componente importante de esas leyes. La Ley Modelo de la CNUDMI sobre Comercio Electrónico ha pasado a ser la norma más influyente en las leyes que se promulgan en la materia y su amplia aplicación ha ayudado a promover en gran medida la armonización internacional. La ratificación amplia de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales promovería aún más la armonización, al ofrecer un conjunto de normas especialmente aplicables a las operaciones internacionales.

235. La adopción de esas normas de la CNUDMI también redundaría en beneficio de la utilización internacional de métodos de autenticación y firma electrónicas. En particular, los criterios flexibles de equivalencia funcional entre las firmas electrónicas y las firmas sobre papel previstos en la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales pueden servir de marco común internacional para que los métodos de autenticación

[314] India, Ley de tecnología de la información, 2000, artículo 42, párrafo 2; y Turquía, Ordenanza sobre los procedimientos y principios relativos a la aplicación de la Ley sobre la firma electrónica (2005), artículo 15 *f)* e *i)*.

[315] Islas Caimán, Ley de operaciones electrónicas (2000), artículo 31 *b)*; China, Ley sobre las firmas electrónicas, artículo 15; Tailandia, Ley de operaciones electrónicas (2001), artículo 27, párrafo 2; y Viet Nam, Ley de operaciones electrónicas, artículo 25, párrafo 2 *b)*.

[316] China, Ley sobre las firmas electrónicas, artículo 27; Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, artículo 17 *e)*; Federación de Rusia, Ley Federal sobre las firmas digitales electrónicas (2002), cláusula 12, párrafo 2; Panamá, Ley de firma digital (2001), artículo 39; República Dominicana, Ley sobre comercio electrónico, documentos y firmas digitales (2002), artículo 55; y Venezuela (República Bolivariana de), Ley sobre mensajes de datos y firmas electrónicas, artículo 40.

y firma electrónicas cumplan los requisitos extranjeros de forma con respecto a las firmas. Aún así, pueden persistir los problemas, en particular en relación con la utilización internacional de métodos de autenticación y firma electrónicas que entrañen la participación de un tercero de confianza en el proceso de autenticación o de firma.

236. Los problemas que se plantean en esta esfera en particular se derivan en gran medida de la falta de uniformidad de las normas técnicas o de la incompatibilidad del equipo o los programas informáticos, lo que da lugar a que no exista la interoperabilidad internacional. Todo esfuerzo que se haga por armonizar las normas y aumentar la compatibilidad técnica puede ayudar a solucionar las dificultades que se presentan actualmente. No obstante, también hay dificultades jurídicas relacionadas con la utilización de métodos de autenticación y firma electrónicas, en particular en relación con algunas leyes nacionales que prescriben o favorecen la utilización de una tecnología determinada para las firmas electrónicas, normalmente la tecnología de firma digital.

237. En las leyes que reconocen valor jurídico a las firmas digitales normalmente se asigna el mismo valor jurídico a las firmas respaldadas por certificados extranjeros únicamente en la medida en que se consideran equivalentes a los certificados nacionales. Del análisis realizado para el presente estudio se desprende que, para determinar debidamente la equivalencia jurídica, es necesario comparar no solo las normas técnicas y de seguridad de una tecnología de firma en particular, sino también las normas jurídicas que regirían la responsabilidad de las diversas partes interesadas. La Ley Modelo de la CNUDMI sobre Firmas Electrónicas proporciona un conjunto de normas comunes básicas para regular ciertos deberes de las partes interesadas en el proceso de autenticación y firma que pueden influir en su responsabilidad individual. También existen textos regionales, como la Directiva de la Unión Europea sobre la firma electrónica, que ofrecen un marco legislativo análogo aplicable al régimen de responsabilidad de los prestadores de servicios de certificación que actúan en la región. Sin embargo, ninguno de esos textos aborda todas las cuestiones relativas a la responsabilidad suscitadas por la utilización internacional de ciertos métodos de autenticación y firma electrónicas.

238. Cabe destacar la importancia de que los legisladores y los encargados de formular políticas comprendan las diferencias que existen entre los regímenes de responsabilidad de los diversos países y los elementos comunes a todos ellos, de modo que se puedan idear métodos y procedimientos apropiados para reconocer las firmas respaldadas por certificados extranjeros. Es posible que en varios países las leyes ya den respuestas sustancialmente equivalentes a las diversas cuestiones examinadas en el presente documento de consulta, entre otras cosas por tratarse de países con una tradición jurídica común o que pertenecen a un marco de integración regional. Esos países tal vez consideren conveniente elaborar normas de responsabilidad comunes o incluso armonizar su normativa interna con objeto de facilitar la utilización transfronteriza de métodos de autenticación y firma electrónicas.

United Nations publication
ISBN: 978-92-1-133663-4
Sales No. S.09.V.4

FOR UNITED NATIONS USE ONLY

Printed in Austria
V.08-55701—March 2009—725