Naciones Unidas A/CN.9/630/Add.5

Asamblea General

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

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

Posible labor futura en la esfera del comercio electrónico

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

Nota de la Secretaría

Adición

En el anexo de la presente nota figura la última parte de un modelo de capítulo sobre cuestiones jurídicas relacionadas con la utilización internacional de métodos de autenticación y firma electrónicas.

V.07-82299 (S) 230507 240507

Anexo

Índice

Segunda parte

Utilización transfronteriza de métodos de autenticación y firma electrónicas (*continuación*)

[...]

II. Métodos y criterios para establecer la equivalencia jurídica

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

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

1. 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[1]. 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.

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

2. 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[2].

3. 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.

---

[1] Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase la nota [...]), artículo 9, párrafo 1, apartados a) y b).

[2] Smedinghoff (véase la nota [...]), sección 3.2.1.

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[3].

4. 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

5. 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.

6. 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 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[4].

7. 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

[3] Ibíd.
[4] Ibíd.

extender un certificado a una persona imaginaria, en cuyo caso sólo resultarían perjudicadas las partes que confiaran en él[5].

8. 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[6], si bien en algunos países la norma parece haberse hecho más estricta y, en lugar de "diligencia razonable", se exigen mayores garantías[7].

9. 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 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[8].

10. 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[9], o garantiza su exactitud[10], si bien en algunos de esos países puede

---

[5] Ibíd.

[6] 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).

[7] 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.

[8] Directiva de la Unión Europea sobre la firma electrónica (véase la nota [...]), artículo 6, párrafo 1.

[9] 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 (China), Ordenanza sobre operaciones electrónicas, artículo 39; India, Ley sobre tecnología de la información, 2000, artículo 36 e); Mauricio, Ley sobre operaciones

condicionar esa garantía formulando la declaración correspondiente en el certificado[11]. 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[12].

11. 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[13] o de mantener sistemas de respaldo de la información relativa a los certificados[14]. 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[15]. 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[16] o expida el certificado conforme a lo acordado con el suscriptor[17]. 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[18].

12. 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"[19]. 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

---

electrónicas, 2000, artículo 27, párrafo 2) d), y Singapur, Ley de operaciones electrónicas, artículo 29 2) a) y c) y artículo 30 1).

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

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

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

[13] Ibíd, 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.

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

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

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

[17] 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).

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

[19] Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase la nota [...]), artículo 8, inciso c) del párrafo 1.

esto se formula imponiendo el deber general de proporcionar información exacta al prestador de servicios de certificación[20] o de actuar con diligencia razonable para garantizar la veracidad de la información[21], y otras veces se declara al firmante expresamente responsable de los daños provocados por el incumplimiento de este deber[22].

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

13. 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.

14. 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 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.

15. 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"[23], 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

---

[20] 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).

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

[22] 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.

[23] Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase la nota [...]), artículo 9, párrafo 1 f).

sistemas fiables[24]. En algunos casos existe el deber específico de adoptar medidas para evitar la falsificación de certificados[25]. 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[26]. 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[27].

16. 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"[28]. 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[29], o declara al firmante único responsable de salvaguardar el dispositivo de creación de firma[30]. No obstante, esa obligación suele estar calificada como deber de ejercer control adecuado sobre el dispositivo de creación de firma o de adoptar medidas adecuadas para ejercer control sobre éste[31], de actuar con diligencia para evitar el uso no autorizado[32], o de actuar con diligencia razonable para evitar que el dispositivo de firma se utilice sin autorización[33].

---

[24] 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 6), y Túnez, *Loi nº2000-83 du 9 août 2000 relative aux échanges et au commerce électronique*, artículo 13.

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

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

[27] Ibíd., artículo 21 p).

[28] Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase la nota [...]), artículo 8, párrafo 1 a).

[29] 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); Turquía, Ordenanza sobre los procedimientos y principios relativos a la aplicación de la Ley de la firma electrónica (2005), artículo 15 e).

[30] Túnez, *Loi relative aux échanges et au commerce électronique*, artículo 21.

[31] 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).

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

[33] 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, 2000 artículo 35 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.

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

17. 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.

18. 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.

19. 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 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"[34]. Si se ofrece ese servicio, el prestador de servicios de certificación está obligado a cerciorarse de que ese servicio exista[35].

20. 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

---

[34] Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase la nota [...]), artículo 9, párrafo 1 d), v) y vi).

[35] Ibíd., artículo 9, párrafo 1 e).

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[36]. En algunas legislaciones nacionales se obliga al prestador de servicios de certificación a adoptar medidas para impedir la falsificación de certificados[37] o a revocar el certificado inmediatamente después de que se determine que estaba basado en información inexacta o falsa[38].

21. 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"[39].

22. 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[40], si bien en algunos casos la ley únicamente obliga al firmante a comunicar ese hecho al prestador de servicios de certificación[41]. 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[42]. 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

---

[36] Directiva de la Unión Europea sobre la firma electrónica, (véase la nota [...]), artículo 6 , párrafo 2; véase también el párrafo b) anexo II de la Directiva.

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

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

[39] Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase la nota [...]), artículo 8, párrafo 1 b) i) y ii).

[40] 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 (2002) sobre las firmas digitales electrónicas, 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.

[41] 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).

[42] Islas Caimán, Ley de operaciones electrónicas, 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).

oportuno aviso de la pérdida del control de la clave privada o si no solicita la revocación del certificado[43].

Conclusión

23. 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.

24. 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[44] 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[45] promovería aún más la armonización, al ofrecer un conjunto de normas especialmente aplicables a las operaciones internacionales.

25. 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 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.

26. 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

---

[43] 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.

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

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

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.

27. 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 sólo 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.

28. 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.