Naciones Unidas A/CN.9/630/Add.4

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 internacional de métodos de autenticación y firma electrónicas

Nota de la Secretaría

Adición

En el anexo de la presente nota figura una parte (las secciones A y B.1 del capítulo II de la segunda parte) de un modelo de capítulo de un documento de consulta sobre las cuestiones jurídicas relativas a la utilización internacional de métodos de autenticación y firma electrónicas.

V.07-82268 (S) 220507 230507

Anexo

Índice

		Párrafos	*Página*
Segunda parte	Utilización transfronteriza de métodos de firma y autenticación electrónicas (*continuación*)		
II.	Métodos y criterios para establecer la equivalencia jurídica	1-50	3
A.	Tipos y mecanismos de reconocimiento recíproco	3-12	3
1.	Reconocimiento recíproco	5-8	4
2.	Certificación recíproca entre infraestructuras de clave pública	9-12	5
B.	Equivalencia de las normas de conducta y los regímenes de responsabilidad	13-72	6
1.	Base de responsabilidad en el marco de una infraestructura de clave pública	17-50	9

Segunda parte

Utilización transfronteriza de métodos de firma y autenticación electrónicas

[...]

II. Métodos y criterios para establecer la equivalencia jurídica

1. 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[1]. 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.

2. 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 tercero 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.

A. Tipos y mecanismos de reconocimiento recíproco

3. 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[2]. Por ejemplo, las leyes relativas

---

[1] Véase la nota [...] [*The Use of Authentication across Borders in OECD Countries*].

[2] 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,

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.

4. 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

5. 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[3]. 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 zona de la ICP correspondiente[4]. 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.

6. 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

---

http://www.biac.org/statements/iccp/AGBtoWTOApril1999.pdf, consultado el 5 de febrero de 2007, pág. 29.

[3] El concepto de reconocimiento recíproco fue elaborado en 2000 por el entonces llamado *Electronic Authentication Task Group* del entonces llamado *Asia-Pacific Economic Cooperation Telecomunications 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), que puede consultarse en http://www.apec.org/apec/publications/all_publications/telecommunications.html, consultado el 7 de febrero de 2007.

[4] 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.

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.

7. 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.

8. 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[5] y las declaraciones de prácticas en materia de certificación[6], 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 de certificación o en la declaración de prácticas de certificación del dominio de ICP extranjero.

2. Certificación recíproca entre infraestructuras de clave pública

9. 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.

---

[5] Una política de certificación es un conjunto determinado de normas en que se establece la aplicabilidad de un certificado a una comunidad o clase determinada de aplicaciones con requisitos de seguridad comunes.

[6] 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.

10. 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.

11. 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.

12. 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

13. 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[7]. 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.

14. 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

[7] Por ejemplo, el Grupo de trabajo sobre política 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 20 de febrero de 2007).

analizaron (véase *supra*, párrafos [... a ...]. 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.

15. 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 tenido 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*)[8] de 2000 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 mayoría de los demás foros que adoptan un enfoque minimalista de la firma electrónica, como Australia[9];

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[10], 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

---

[8] Véase la nota [...] [Código de los Estados Unidos, título 15, capítulo 96, sección 7031 (*Principles governing the use of electronic signatures in international transactions*)].

[9] 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 el *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, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf, consultado el 7 de febrero de 2007, págs. 43 a 47).

[10] Véase la nota [...], [*Diario Oficial de las Comunidades Europeas*, L 13/12].

por ahora significa únicamente firmas digitales basadas en la infraestructura de clave pública[11];

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[12], 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.

16. 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 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.

---

[11] 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, sección 4.

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

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

17. 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[13]. 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.

18. Se desprende de lo anterior que el régimen de la responsabilidad varía no sólo 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 *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

19. 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[14].

---

[13] 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,* 2002, Nº 1. (http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/hindelang, consultado el 6 de febrero de 2007), examina en detalle, en la sección 4.1.1, la posibilidad de crear una relación contractual entre el prestador de servicios de certificación y el tercero conforme al derecho inglés, llegando a una conclusión negativa. Sin embargo, hay foros en que podría establecerse una relación contractual.

[14] Con respecto al examen del régimen de responsabilidad en este contexto, véase Balboni, "*Liability of certification service providers ...*" (véase la nota [...]), págs. 232 y sigs.

i) Negligencia simple

20. 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.

21. 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[15]. Pueden utilizarse varios elementos para evaluar el cumplimiento por los prestadores de servicios de certificación de la norma general en materia de diligencia[16]. 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[17]. La Ley Modelo aplica la misma norma general en materia de diligencia

---

[15] Véase la nota [...] [publicación de las Naciones Unidas, Nº de venta S.02.V.8]. 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: (...).".

[16] Véase la nota [...] [*Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno, 2001*]. 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 sobre conflictos de leyes".

[17] Véase la nota [...] [publicación de las Naciones Unidas, Nº de venta S.02.V.8]. El artículo 8 de la Ley Modelo dispone lo siguiente: Cuando puedan utilizarse datos de creación de firmas para

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[18].

22. Unos pocos países, por lo general Estados promulgantes de la Ley Modelo de la CNUDMI sobre Comercio Electrónico[19], han adoptado la norma general de "diligencia razonable" en lo tocante al proceder del prestador de servicios de certificación[20]. 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[21]. Ciertamente, como se expone más abajo (véase el párr. 29), tal parece ser el caso en la mayoría de los países.

23. 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"[22]. En varios países la ley va acompañada de una lista más o menos extensa de obligaciones positivas, sin exponer el grado de diligencia previsto ni indicar las consecuencias del incumplimiento de esas obligaciones[23]. Sin embargo,

---

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.".

[18] Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase la nota [...]), apartado a) del artículo 11 e incisos i) y ii) del apartado b) del artículo 11.

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

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

[21] "*Certification authority*: *liability issues*", preparado para la American Bankers Association por Thomas J. Smedinghoff, febrero de 1998 (http://www.bakernet.com/ecommerce/CA-Liability-Analysis.doc), consultado el 5 de febrero de 2007, sección 1.1.

[22] Por ejemplo, la Ley de operaciones electrónicas (2001), artículo 27, de Tailandia.

[23] Por ejemplo, la 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; Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos,* artículo 17; India, Ley de la tecnología de la información, 2000, artículos 40 a 42; Islas Caimán, Ley de operaciones electrónicas, 2000, sección 31; Mauricio, Ley de operaciones electrónicas, 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 (2005), artículo 15; y Venezuela (República Bolivariana de), *Ley sobre mensajes de datos y firmas electrónicas*, artículo 19.

en algunos países la ley complementa expresamente la lista de obligaciones con una declaración general de responsabilidad del firmante por su eventual incumplimiento[24], que en un caso es incluso de carácter penal[25]. 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[26].

24. 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 confía[27]. Sin embargo, en algunos casos, este requisito no se indica expresamente[28]. 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

---

[24] China, Ley de firmas electrónicas, 2004, artículo 27; Colombia, *Ley 527 sobre comercio electrónico*, artículo 40; México, *Código de Comercio: Decreto sobre firma electrónica (2003)*, artículo 99; República Dominicana, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, artículos 53 y 55; Panamá, *Ley de firma digital, 2001*, artículos 37 y 39; Federación de Rusia, Ley federal sobre firmas electrónicas digitales (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.

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

[26] 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.

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

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

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

25. 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.

26. En los ordenamientos de tradición romanista puede producirse una presunción de falta en relación con la responsabilidad por incumplimiento de contrato[29] 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.

27. 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 actuar como miembros de su profesión, y tienen la obligación de actuar como lo haría un miembro razonable de la profesión en cualquier circunstancia[30]. 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

---

[29] 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 (*"Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat"*). 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 (*"Lorsque le créancier ne peut obtenir l'exécution de l'obligation ou ne peut l'obtenir qu'imparfaitement, le débiteur est tenu de réparer le dommage en résultant, à moins qu'il ne prouve qu'aucune faute ne lui est imputable"*). 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 (*obligation de résultat*), pero debe determinarse que ha habido negligencia si el objeto del contrato era ofrecer un nivel de ejecución (*obligation de moyen*), y no un resultado concreto (véase Gérard Légier, "Responsabilité contractuelle", *Répertoire de droit civil Dalloz*, agosto de 1989, Nº 58-68).

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

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[31].

28. 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.

29. 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[32]. 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).

30. 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 obligaciones legales[33]. No está en absoluto claro si todos esos ordenamientos jurídicos invierten la carga de la prueba, pero algunos de ellos sí

---

[31] "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)).

[32] Véase la nota [...] [*Diario Oficial de las Comunidades Europeas*, L 13/12]. 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..." (véase la nota […]), pág. 222).

[33] 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.

prevén explícitamente esa inversión, bien de manera general[34], o bien para obligaciones concretas[35].

31. 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

32. 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.

33. 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 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

---

[34] China, Ley de firmas electrónicas (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 (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.”

[35] 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), artículo 23, párrafo 2 b).

de certificación puede quedar exento de responsabilidad si demuestra que actuó con la diligencia debida[36].

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

34. 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.

35. 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.

36. 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[37], con pocas excepciones[38]. En algunos ordenamientos podría establecerse una analogía entre las actividades de un prestador de servicios de certificación y los notarios, que suelen ser considerados

---

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

[37] 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.

[38] 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.

responsables del daño causado por la negligencia cometida en el ejercicio de sus funciones.

37. 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, a menos que exista una disposición legal explícita al respecto[39]. 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"[40], a menos que las palabras negligentes "se comuniquen directamente, con conocimiento u 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"[41].

38. 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[42]:

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;

---

[39] 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* ... (véase la nota [11]), pág. 15.

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

[41] Ibíd., pág. 447.

[42] Smedinghoff, "Certification authority: liability issues" (véase la nota [23]), 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 específico.

39. 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"[43]. 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 que "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[44].

40. 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"[45].

41. 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[46]. 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,

---

[43] *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno* (véase la nota [...]), párr. 150.

[44] Las excepciones son Dinamarca y Hungría (Balboni, "Liability of certification service providers ..." (véase la nota [...]), pág. 220.

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

[46] Smedinghoff, "Certification authority: liability issues" (véase la nota [23]), sección 4.5.

en este caso, están relacionadas con la prueba de la proximidad del daño[47]. 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[48].

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

42. 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[49].

43. 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[50], o se le imponen unas limitaciones claras[51]. 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.

44. 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

---

[47] Dumortier y otros, “The legal and market aspects of electronic signatures” (véase la nota [...]), pág. 215.

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

[49] Véase Smedinghoff, “Certification authority: liability issues” (véase la nota [23]), sección 5.2.5.4; y Hindelang, “No remedy for disappointed trust...” (véase la nota [15]), sección 4.1.1.

[50] 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” (véase la nota [...]), números 262 y 263).

[51] 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 António Pinto Monteiro, *Cláusulas Limitativas e de Exclusão de Responsabilidade Civil*, (Coimbra, Faculdade de Direito de Coimbra, 1985), pág. 217).

no 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”[52] 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”[53]. 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[54]. 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[55].

45. 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.

46. 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[56], 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

---

[52] *First Financial Ins. Co. v. Purolator Security, Inc.*, 388 N.E.2d 17, 22 (Tribunal de Apelaciones 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” (véase la nota [23]), sección 5.2.5.4.

[53] Ibíd., citando a *Williams v.Walker-Thomas Furniture Co.*, 350 F.2d 315, 320 (D.C. 1965), citado en Smedinghoff, "Certification authority: liability issues" (véase la nota [23]), sección 5.2.5.4.

[54] *First Financial Ins. Co. v. Purolator Security, Inc*., 388 N.E.2d 17, 22 (Tribunal de Apelaciones del Primer Distrito de Illinois, 1979), citado en Smedinghoff, “Certification authority: liability issues” (véase la nota [23]), sección 5.2.5.4.

[55] Raymond T. Nimmer, *Information Law*, sección 11.12[4][a], págs. 11 a 37, citado en Smedinghoff, "Certification authority: liability issues" (véase la nota [23]), sección 5.2.5.4.

[56] 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 8 de febrero de 2007).

el firmante tenga todavía menos posibilidades de 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[57]. 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.

47. 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"[58]. 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"[59]. 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"[60]. 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[61].

48. 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[62]. 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.

49. En otros ordenamientos jurídicos nacionales se apoyan esas prácticas contractuales admitiendo un límite a la responsabilidad de los prestadores de

---

[57] Sneddon, "*Legal liability and e-transactions* ..." (véase la nota [11]), pág. 18.

[58] Directiva de la Unión Europea sobre la firma electrónica (véase la nota [...]), artículo 6, párrafo 3.

[59] Ibíd.

[60] Ibíd., artículo 6, párrafo 4.

[61] Ibíd.

[62] Dumortier y otros, "The legal and market aspects of electronic signatures" (véase la nota [...]), pág. 55, y el examen al respecto en Hindelang, "No remedy for disappointed trust ..." (véase la nota [15]), 4.1.1. Balboni, "Liability of certification service providers ..." (véase la nota [...]), 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".

servicios de certificación frente a cualquier parte potencialmente afectada. Por lo general esas leyes 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[63]. 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[64], 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[65].

50. 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[66].

---

[63] Argentina, Ley de firma digital (2001), artículo 39; Barbados, capítulo 308B, Ley de operaciones electrónicas (1998), artículo 20, párrafos 3 y 4; Bermuda, 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).

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

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

[66] En el caso de Australia, véase Sneddon, *Legal liability and e-transactions* (véase la nota [11]), págs. 44 a 47; en cuanto a los Estados Unidos, véase Smedinghoff, "Certification authority: liability issues" (véase la nota [23]), sección 5.2.51.