Naciones Unidas A/CN.9/1112

Asamblea General

Distr. general
21 de febrero de 2022
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
55º período de sesiones
Nueva York, 27 de junio a 15 de julio de 2022

Proyecto de ley modelo sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza

Nota de la Secretaría

1. En su 62º período de sesiones (Viena, 22 a 26 de noviembre de 2021), el Grupo de Trabajo IV (Comercio Electrónico) concluyó su tercera lectura del proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza y su nota explicativa.

2. En ese período de sesiones, el Grupo de Trabajo solicitó a la secretaría que revisara el proyecto de disposiciones y la nota explicativa para que reflejaran sus deliberaciones y decisiones y que remitiera el texto revisado a la Comisión, en forma de ley modelo, para que esta lo examinara en su 55º período de sesiones, en 2022. También se pidió a la secretaría que transmitiera el texto revisado a todos los Gobiernos y organizaciones internacionales pertinentes para que formularan observaciones, y que recopilara las observaciones recibidas a fin de someterlas a consideración de la Comisión (A/CN.9/1087, párr. 11).

3. El texto revisado del proyecto de ley modelo figura en el anexo I del presente documento y la versión revisada de la nota explicativa en el anexo II. Las modificaciones introducidas reflejan las deliberaciones sostenidas por el Grupo de Trabajo en su 62º período de sesiones, tal como se informa en el documento A/CN.9/1087.

V.22-00941 (S) 310322 310322

Anexo I

Proyecto de ley modelo sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza

Capítulo I. Disposiciones generales

Artículo 1. Definiciones

A los efectos de la presente Ley:

a) Por “atributo” se entenderá un elemento de información o datos vinculados a una persona;

b) Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares;

c) Por “identificación electrónica” [“autenticación”], en el contexto de los servicios de gestión de la identidad, se entenderá un proceso utilizado para obtener una garantía suficiente de la vinculación entre una persona y una identidad;

d) Por “identidad” se entenderá un conjunto de atributos que permiten distinguir a una persona de manera inequívoca en un contexto particular;

e) Por “credenciales de identidad” se entenderán los datos, o el objeto físico en el que pueden residir los datos, que una persona puede presentar para la identificación electrónica;

f) Por “servicios de gestión de la identidad” se entenderán los servicios que consisten en gestionar la comprobación de la identidad o la identificación electrónica;

g) Por “proveedor de servicios de gestión de la identidad” se entenderá toda persona que celebre un acuerdo con un usuario para la prestación de servicios de gestión de la identidad;

h) Por “sistema de gestión de la identidad” se entenderá un conjunto de funciones y capacidades utilizadas para gestionar la comprobación de la identidad y la identificación electrónica;

i) Por “comprobación de la identidad” se entenderá el proceso de reunión, verificación y validación de atributos que sean suficientes para definir y confirmar la identidad de una persona en un contexto determinado;

j) Por “parte que confía” se entenderá toda persona que actúe en función del resultado de un servicio de gestión de la identidad o un servicio de confianza;

k) Por “usuario” se entenderá toda persona que celebre un acuerdo con un proveedor de servicios de gestión de la identidad o un proveedor de servicios de confianza para la prestación de servicios de gestión de la identidad o servicios de confianza;

l) Por “servicio de confianza” se entenderá un servicio electrónico que ofrece garantías de determinadas propiedades de un mensaje de datos e incluye los métodos para crear y gestionar firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, autenticación de sitios web, archivado electrónico y servicios de entrega electrónica certificada;

m) Por “proveedor de servicios de confianza” se entenderá toda persona que celebre un acuerdo con un usuario para la prestación de uno o varios servicios de confianza.

Artículo 2. Ámbito de aplicación

1. La presente Ley será aplicable a la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza en el contexto de actividades comerciales y servicios relacionados con el comercio.

2. Nada de lo dispuesto en la presente Ley impondrá la obligación de identificar a una persona.

3. Nada de lo dispuesto en la presente Ley afectará a obligación legal alguna de identificar a una persona o utilizar un servicio de confianza de conformidad con un procedimiento definido o establecido en la ley.

4. Salvo en los casos previstos en la presente Ley, nada de lo dispuesto en ella afectará a la aplicación a los servicios de gestión de la identidad o a los servicios de confianza de cualquier ley que sea aplicable a la protección y la privacidad de los datos.

Artículo 3. Utilización voluntaria de la gestión de la identidad y los servicios de confianza

1. Nada de lo dispuesto en la presente Ley obligará a persona alguna a utilizar un servicio de gestión de la identidad o un servicio de confianza o a utilizar un determinado servicio de gestión de la identidad o un determinado servicio de confianza sin su consentimiento.

2. A los efectos de lo dispuesto en el párrafo 1, el consentimiento de una persona podrá inferirse de su conducta.

Artículo 4. Interpretación

1. En la interpretación de la presente Ley se tendrán en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y la observancia de la buena fe en el comercio internacional.

2. Las cuestiones relativas a las materias que se rigen por la presente Ley que no estén expresamente resueltas en ella se dirimirán de conformidad con los principios generales en que esta se basa.

Capítulo II. Gestión de la identidad

Artículo 5. Reconocimiento jurídico de la gestión de la identidad

A reserva de lo dispuesto en el artículo 2, párrafo 3, no se negarán efectos jurídicos, validez, fuerza ejecutoria ni admisibilidad como prueba a la identificación electrónica por la sola razón:

a) de que la comprobación de la identidad y la identificación electrónica estén en forma electrónica, o

b) de que el sistema de gestión de la identidad no haya sido designado de conformidad con el artículo 11.

Artículo 6. Obligaciones de los proveedores de servicios de gestión de la identidad

Todo proveedor de servicios de gestión de la identidad deberá, como mínimo:

a) tener en vigor normas operacionales, políticas y prácticas que resulten apropiadas para los fines y el diseño del sistema de gestión de la identidad y que permitan definir, como mínimo, los requisitos que deberán cumplirse a los siguientes efectos:

i) inscribir personas, en particular mediante:

a. el registro y la reunión de atributos;

b. la comprobación y verificación de la identidad, y

c. la vinculación de las credenciales de identidad a la persona;

ii) actualizar atributos;

iii) gestionar credenciales de identidad, en particular mediante:

a. la emisión, entrega y activación de credenciales;

b. la suspensión, revocación y reactivación de credenciales, y

c. la renovación y sustitución de credenciales;

iv) gestionar la identificación electrónica de personas, en particular mediante:

a. la gestión de factores de identificación electrónica, y

b. la gestión de mecanismos de identificación electrónica;

b) actuar de conformidad con sus normas operacionales, políticas y prácticas y de acuerdo con las declaraciones que haya hecho al respecto;

c) garantizar la disponibilidad en línea y el correcto funcionamiento del sistema de gestión de la identidad;

d) facilitar el acceso de los usuarios y los terceros a sus normas operacionales, políticas y prácticas;

e) proporcionar a la parte que confía medios fácilmente accesibles que le permitan determinar, cuando proceda:

i) cualquier limitación que exista respecto de los fines o el valor para los que puede utilizarse el servicio de gestión de la identidad, y

ii) cualquier limitación que haya establecido el proveedor de servicios de gestión de la identidad con respecto al alcance o la magnitud de la responsabilidad, y

f) proporcionar y poner a disposición del público los medios que puede emplear un usuario para notificar una falla de seguridad al proveedor de servicios de gestión de la identidad de conformidad con el artículo 8.

Artículo 7. Obligaciones de los proveedores de servicios de gestión de la identidad en caso de violación de los datos

1. En el caso de que se produzca una falla de seguridad o una pérdida de integridad que tenga un impacto considerable en el sistema de gestión de la identidad, incluidos los atributos que en él se gestionan, el proveedor de los servicios de gestión de la identidad deberá, de conformidad con la ley:

a) tomar todas las medidas razonables para contener la falla o la pérdida, entre ellas, cuando proceda, la suspensión del servicio afectado o la revocación de las credenciales de identidad afectadas;

b) subsanar la falla o la pérdida, y

c) notificar la falla o la pérdida.

2. Si una persona notifica una falla de seguridad o una pérdida de integridad al proveedor de los servicios de gestión de la identidad, este deberá:

a) investigar la posible falla o pérdida, y

b) adoptar cualquier otra medida que corresponda conforme a lo dispuesto en el párrafo 1.

Artículo 8. Obligaciones de los usuarios

El usuario deberá notificar al proveedor de los servicios de gestión de la identidad utilizando alguno de los medios que este le hubiera proporcionado de conformidad con el artículo 6, o empleando otros medios razonables de notificación, en los siguientes casos:

a) cuando el usuario sepa que sus credenciales de identidad se han visto comprometidas, o

b) cuando las circunstancias de que tenga conocimiento el usuario den lugar a un riesgo considerable de que sus credenciales de identidad puedan haberse visto comprometidas.

Artículo 9. Identificación de personas mediante la gestión de la identidad

A reserva de lo dispuesto en el artículo 2, párrafo 3, cuando la ley requiera la identificación de una persona con un fin determinado, o prevea consecuencias para el caso de que se omita la identificación, ese requisito se dará por cumplido respecto de los servicios de gestión de la identidad si se utiliza un método para realizar la identificación electrónica de la persona con ese fin.

Artículo 10. Requisitos de fiabilidad de los servicios de gestión de la identidad

1. A los efectos de lo dispuesto en el artículo 9, el método deberá:

a) ser tan fiable como resulte apropiado para los fines para los que se utiliza el servicio de gestión de la identidad, o

b) haber demostrado en la práctica que ha cumplido la función que se describe en el artículo 9.

2. Para determinar la fiabilidad del método deberán tenerse en cuenta todas las circunstancias pertinentes, que podrán ser, entre otras, las siguientes:

a) el cumplimiento por el proveedor de servicios de gestión de la identidad de las obligaciones establecidas en el artículo 6;

b) la conformidad de las normas operacionales, políticas y prácticas del proveedor de servicios de gestión de la identidad con cualesquiera normas y procedimientos internacionales reconocidos que sean aplicables y que resulten pertinentes para la prestación de servicios de gestión de la identidad, incluidos los marcos de niveles de garantía, en particular las normas relativas a los siguientes aspectos;

i) la gobernanza;

ii) la publicación de anuncios y la información que se facilita al usuario;

iii) la gestión de la seguridad de la información;

iv) el mantenimiento de registros;

v) la infraestructura y el personal;

vi) las inspecciones técnicas, y

vii) las actividades de supervisión y auditoría;

c) toda supervisión o certificación que se hubiera realizado con respecto al servicio de gestión de la identidad;

d) cualquier nivel de fiabilidad del método utilizado que resulte pertinente;

e) el fin para el que se utilice la identificación, y

f) cualquier acuerdo pertinente entre las partes, incluida cualquier limitación respecto de los fines o el valor de las operaciones para las que pudiera utilizarse el servicio de gestión de la identidad.

3. A los efectos de determinar la fiabilidad del método, no se tomará en consideración:

a) la ubicación geográfica del lugar en que se preste el servicio de gestión de la identidad, ni

b) la ubicación geográfica del establecimiento del proveedor de servicios de gestión de la identidad.

4. Se presumirá que el método utilizado por un servicio de gestión de la identidad designado de conformidad con el artículo 11 es fiable.

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

a) demuestre de cualquier otra manera la fiabilidad de un método, o

b) presente pruebas de que un método utilizado por un servicio de gestión de la identidad designado de conformidad con el artículo 11 no es fiable.

Artículo 11. Designación de servicios de gestión de la identidad fiables

1. [*La persona, el órgano o la entidad, de carácter público o privado, a que la jurisdicción promulgante haya atribuido competencia expresamente*] podrá designar servicios de gestión de la identidad que se presuman fiables.

2. [*La persona, el órgano o la entidad, de carácter público o privado, a que la jurisdicción promulgante haya atribuido competencia expresamente*] deberá:

a) tener en cuenta todas las circunstancias pertinentes, incluidos los factores mencionados en el artículo 10, al designar un servicio de gestión de la identidad, y

b) publicar una lista de servicios de gestión de la identidad designados, que incluya detalles de los proveedores de esos servicios.

3. Toda designación que se realice de conformidad con el párrafo 1 deberá ajustarse a las normas y procedimientos internacionales reconocidos que sean pertinentes para llevar a cabo el proceso de designación, incluidos los marcos de niveles de garantía.

4. A los efectos de designar un servicio de gestión de la identidad, no se tomará en consideración:

a) la ubicación geográfica del lugar en que se preste el servicio de gestión de la identidad, ni

b) la ubicación geográfica del establecimiento del proveedor de servicios de gestión de la identidad.

Artículo 12. Responsabilidad de los proveedores de servicios de gestión de la identidad

1. El proveedor de servicios de gestión de la identidad que incumpla las obligaciones que le imponen los artículos 6 y 7 deberá responder de las pérdidas que dicho incumplimiento cause al usuario o a la parte que confía.

2. El párrafo 1 se aplicará de conformidad con las normas de responsabilidad establecidas en la ley y sin perjuicio de lo siguiente:

a) la existencia de cualquier otro fundamento de la responsabilidad previsto en la ley, incluida la responsabilidad por incumplimiento de las obligaciones contractuales, o

b) cualquier otra consecuencia jurídica que se derive del incumplimiento por el proveedor de servicios de gestión de la identidad de las obligaciones que le impone la presente Ley.

3. No obstante lo dispuesto en el párrafo 1, el proveedor de servicios de gestión de la identidad no responderá ante el usuario de las pérdidas que se deriven de la utilización de un servicio de gestión de la identidad:

a) en la medida en que el uso realizado exceda las limitaciones establecidas en cuanto a los fines o el valor de la operación para la que se utilice el servicio de gestión de la identidad, y

b) siempre y cuando esas limitaciones estén previstas en el acuerdo existente entre el proveedor de servicios de gestión de la identidad y el usuario.

4. No obstante lo dispuesto en el párrafo 1, el proveedor de servicios de gestión de la identidad no responderá ante una parte que confía de las pérdidas que se deriven de la utilización de un servicio de gestión de la identidad:

a) en la medida en que el uso realizado exceda las limitaciones establecidas en cuanto a los fines o el valor de la operación para la que se utilice el servicio de gestión de la identidad, y

b) siempre y cuando el proveedor de servicios de gestión de la identidad haya cumplido las obligaciones que le impone el artículo 6, apartado e), respecto de esa operación.

Capítulo III. Servicios de confianza

Artículo 13. Reconocimiento jurídico de los servicios de confianza

No se negarán efectos jurídicos, validez, fuerza ejecutoria, ni admisibilidad como prueba al resultado de la utilización de un servicio de confianza por la sola razón:

a) de que esa información esté en forma electrónica, o

b) de que el servicio de confianza no haya sido designado de conformidad con el artículo 23.

Artículo 14. Obligaciones de los proveedores de servicios de confianza

1. Todo proveedor de servicios de confianza deberá, como mínimo:

a) tener en vigor normas operacionales, políticas y prácticas que resulten apropiadas para los fines y el diseño del servicio de confianza, incluido un plan para garantizar la continuidad en caso de cese de la actividad;

b) actuar de conformidad con sus normas operacionales, políticas y prácticas y de acuerdo con las declaraciones que haya hecho al respecto;

c) facilitar el acceso de los usuarios y los terceros a sus normas operacionales, políticas y prácticas;

d) proporcionar y poner a disposición del público los medios que puede emplear un usuario para notificar una falla de seguridad al proveedor de servicios de confianza de conformidad con el artículo 15, y

e) proporcionar a la parte que confía medios fácilmente accesibles que le permitan determinar, cuando proceda:

i) cualquier limitación que exista respecto de los fines o el valor para los que puede utilizarse el servicio de confianza, y

ii) cualquier limitación que haya establecido el proveedor de servicios de confianza con respecto al alcance o la magnitud de la responsabilidad.

2. En el caso de que se produzca una falla de seguridad o una pérdida de integridad que tenga un impacto considerable en un servicio de confianza, el proveedor de ese servicio deberá, de conformidad con la ley:

a) tomar todas las medidas razonables para contener la falla o la pérdida, incluida, cuando proceda, la suspensión o la revocación del servicio afectado;

b) subsanar la falla o la pérdida, y

c) notificar la falla o la pérdida.

Artículo 15. Obligaciones de los usuarios

El usuario deberá notificar al proveedor de servicios de confianza utilizando alguno de los medios que este le hubiere proporcionado de conformidad con el artículo 14, párrafo 1, o empleando otros medios razonables de notificación, en los siguientes casos:

a) cuando el usuario sepa que los datos o los medios empleados por el usuario para acceder al servicio de confianza y utilizarlo se han visto comprometidos, o

b) cuando las circunstancias de que tenga conocimiento el usuario den lugar a un riesgo considerable de que el servicio de confianza se haya podido ver comprometido.

Artículo 16. Firmas electrónicas

Cuando la ley requiera la firma de una persona, o prevea consecuencias para el caso de que falte una firma, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

a) para identificar a la persona, y

b) para indicar la voluntad que tiene esa persona respecto de la información contenida en el mensaje de datos.

Artículo 17. Sellos electrónicos

Cuando la ley requiera que una persona jurídica estampe un sello, o prevea consecuencias para el caso de que falte un sello, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

a) para proporcionar una garantía fiable del origen del mensaje de datos, y

b) para detectar cualquier alteración del mensaje de datos que se haya producido después de la fecha y hora en que fue estampado el sello y que no consista en la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación.

Artículo 18. Sellos de tiempo electrónicos

Cuando la ley requiera que un documento en papel o electrónico o cierta información o datos se vinculen a una fecha y hora, o prevea consecuencias para el caso de que falte la fecha y hora, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

a) para indicar la fecha y hora, incluso especificando el huso horario utilizado, y

b) para vincular dicha fecha y hora al mensaje de datos.

Artículo 19. Archivado electrónico

Cuando la ley requiera que se conserve un documento en papel o electrónico o cierta información, o prevea consecuencias para el caso de que no se conserve, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

a) para hacer accesible la información contenida en el mensaje de datos a fin de que pueda consultarse posteriormente;

b) para indicar la fecha y hora de archivado y vincular esa fecha y hora al mensaje de datos;

c) para conservar el mensaje de datos en el formato en que se haya generado, enviado o recibido, o en otro formato que pueda demostrarse que es capaz de detectar cualquier alteración del mensaje de datos que se haya producido con posterioridad a esa fecha y hora y que no consista en la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación, y

d) para conservar, si la hubiera, la información que permita determinar el origen y el destino del mensaje de datos y la fecha y hora en que fue enviado o recibido.

Artículo 20. Servicios de entrega electrónica certificada

Cuando la ley requiera que un documento en papel o electrónico o cierta información se entregue mediante correo certificado u otro servicio similar, o prevea consecuencias para el caso de que no se entregue, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

a) para indicar la fecha y hora en que el mensaje de datos fue recibido para la entrega, y la fecha y hora en que fue entregado;

b) para detectar cualquier alteración del mensaje de datos que se haya producido después de la fecha y hora en que el mensaje de datos fue recibido para la entrega, hasta la fecha y hora en que fue entregado, y que no consista en la adición de algún endoso o de la información exigida en el presente artículo ni en un cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación, y

c) para identificar al remitente y al destinatario.

Artículo 21. Autenticación de sitios web

Cuando la ley requiera la autenticación de un sitio web, o prevea consecuencias para el caso de falta de autenticación de un sitio web, ese requisito se dará por cumplido si se utiliza un método:

a) para identificar a la persona que es titular del nombre de dominio de ese sitio web, y

b) para vincular a esa persona al sitio web.

Artículo 22. Requisitos de fiabilidad de los servicios de confianza

1. A los efectos de lo dispuesto en los artículos 16 a 21, el método deberá:

a) ser tan fiable como resulte apropiado para los fines para los que se utiliza el servicio de confianza, o

b) haber demostrado en la práctica que ha cumplido las funciones que se describen en el artículo.

2. Para determinar la fiabilidad del método deberán tenerse en cuenta todas las circunstancias pertinentes, que podrán ser, entre otras, las siguientes:

a) el cumplimiento por el proveedor de servicios de confianza de las obligaciones establecidas en el artículo 14;

b) la conformidad de las normas operacionales, políticas y prácticas del proveedor de servicios de confianza con cualesquiera normas y procedimientos internacionales reconocidos que sean aplicables y que resulten pertinentes para la prestación de servicios de confianza;

c) cualquier nivel de fiabilidad del método utilizado que resulte pertinente;

d) cualquier norma aplicable del sector;

e) la seguridad de los equipos y programas informáticos;

f) los recursos humanos y financieros, incluida la existencia de activos;

g) la periodicidad y el alcance de las auditorías realizadas por un órgano independiente;

h) la existencia de una declaración de un órgano de supervisión, un órgano de acreditación o un mecanismo voluntario respecto de la fiabilidad del método;

i) el fin para el que se utilice el servicio de confianza, y

j) cualquier acuerdo pertinente entre las partes, incluida cualquier limitación respecto de los fines o el valor de las operaciones para las que pudiera utilizarse el servicio de confianza.

3. A los efectos de determinar la fiabilidad del método, no se tomará en consideración:

a) la ubicación geográfica del lugar en que se preste el servicio de confianza, ni

b) la ubicación geográfica del establecimiento del proveedor del servicio de confianza.

4. Se presumirá que el método utilizado por un servicio de confianza designado de conformidad con el artículo 23 es fiable.

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

a) demuestre de cualquier otra manera la fiabilidad de un método, o

b) presente pruebas de que un método utilizado por un servicio de confianza designado de conformidad con el artículo 23 no es fiable.

Artículo 23. Designación de servicios de confianza fiables

1. [*La persona, el órgano o la entidad, de carácter público o privado, a que la jurisdicción promulgante haya atribuido competencia expresamente*] podrá designar servicios de confianza que se presuman fiables.

2. [*La persona, el órgano o la entidad, de carácter público o privado, a que la jurisdicción promulgante haya atribuido competencia expresamente*] deberá:

a) tener en cuenta todas las circunstancias pertinentes, incluidos los factores mencionados en el artículo 22, al designar un servicio de confianza, y

b) publicar una lista de servicios de confianza designados, que incluya detalles de los proveedores de esos servicios.

3. Toda designación que se realice de conformidad con el párrafo 1 deberá ajustarse a las normas y procedimientos internacionales reconocidos que sean pertinentes para llevar a cabo el proceso de designación.

4. A los efectos de designar un servicio de confianza, no se tomará en consideración:

a) la ubicación geográfica del lugar en que se preste el servicio de confianza, ni

b) la ubicación geográfica del establecimiento del proveedor del servicio de confianza.

Artículo 24. Responsabilidad de los proveedores de servicios de confianza

1. El proveedor de servicios de confianza que incumpla las obligaciones que le impone el artículo 14 deberá responder de las pérdidas que dicho incumplimiento cause al usuario o a la parte que confía.

2. El párrafo 1 se aplicará de conformidad con las normas de responsabilidad establecidas en la ley y sin perjuicio de lo siguiente:

a) la existencia de cualquier otro fundamento de la responsabilidad previsto en la ley, incluida la responsabilidad por incumplimiento de las obligaciones contractuales, o

b) cualquier otra consecuencia jurídica que se derive del incumplimiento por el proveedor de servicios de confianza de las obligaciones que le impone la presente Ley.

3. No obstante lo dispuesto en el párrafo 1, el proveedor de servicios de confianza no responderá ante el usuario de las pérdidas que se deriven de la utilización de un servicio de confianza:

a) en la medida en que el uso realizado exceda las limitaciones establecidas en cuanto a los fines o el valor de la operación para la que se utilice el servicio de confianza, y

b) siempre y cuando esas limitaciones estén previstas en el acuerdo existente entre el proveedor de servicios de confianza y el usuario.

4. No obstante lo dispuesto en el párrafo 1, el proveedor de servicios de confianza no responderá ante una parte que confía de las pérdidas que se deriven de la utilización de un servicio de confianza:

a) en la medida en que el uso realizado exceda las limitaciones establecidas en cuanto a los fines o el valor de la operación para la que se utilice el servicio de confianza, y

b) siempre y cuando el proveedor de servicios de confianza haya cumplido las obligaciones que le impone el artículo 14, párrafo 1 e), respecto de esa operación.

Capítulo IV. Aspectos internacionales

Artículo 25. Reconocimiento transfronterizo de la identificación electrónica

1. La identificación electrónica proporcionada fuera de [*la jurisdicción promulgante*] tendrá en [*dicha jurisdicción*] los mismos efectos jurídicos que tendría la identificación electrónica proporcionada en [*la jurisdicción promulgante*] si el método empleado por el sistema de gestión de la identidad, el servicio de gestión de la identidad o la credencial de identidad, según corresponda, ofrece un nivel de fiabilidad que sea como mínimo equivalente.

2. Para determinar si un sistema de gestión de la identidad, un servicio de gestión de la identidad o una credencial de identidad, según corresponda, ofrece un nivel de fiabilidad que sea como mínimo equivalente, se tomarán en consideración las normas internacionales reconocidas.

3. A los efectos de lo dispuesto en el párrafo 1, se presumirá que un sistema de gestión de la identidad, un servicio de gestión de la identidad o una credencial de identidad ofrecen un nivel de fiabilidad como mínimo equivalente si [*la persona, el órgano o la entidad designados por la jurisdicción promulgante de conformidad con el artículo 11*] ha determinado dicha equivalencia, teniendo en cuenta el artículo 10, párrafo 2.

Artículo 26. Reconocimiento transfronterizo del resultado de la utilización de servicios de confianza

1. El resultado de la utilización de un servicio de confianza prestado fuera de [*la jurisdicción promulgante*] tendrá en [*dicha jurisdicción*] los mismos efectos jurídicos que tendría el resultado de la utilización de un servicio de confianza prestado en [*la jurisdicción promulgante*] si el método empleado por el servicio de confianza ofrece un nivel de fiabilidad que sea como mínimo equivalente.

2. Para determinar si un servicio de confianza ofrece un nivel de fiabilidad que sea como mínimo equivalente, se tomarán en consideración las normas internacionales reconocidas.

3. A los efectos de lo dispuesto en el párrafo 1, se presumirá que el servicio de confianza ofrece un nivel de fiabilidad como mínimo equivalente si [*la persona, el órgano o la entidad designados por la jurisdicción promulgante de conformidad con el artículo 23*] ha determinado dicha equivalencia, teniendo en cuenta el artículo 22, párrafo 2.

Artículo 27. Cooperación

[*La persona, el órgano o la entidad a que la jurisdicción promulgante haya atribuido competencia expresamente*] podrá cooperar con entidades extranjeras mediante el intercambio de información, experiencia y buenas prácticas relacionadas con la gestión de la identidad y los servicios de confianza, en particular con respecto a lo siguiente:

a) el reconocimiento de los efectos jurídicos de los sistemas de gestión de la identidad y servicios de confianza extranjeros, haya sido otorgado unilateralmente o de común acuerdo;

b) la designación de sistemas de gestión de la identidad y servicios de confianza, y

c) la definición de los niveles de garantía de los sistemas de gestión de la identidad y de los niveles de fiabilidad de los servicios de confianza.

Anexo II

Nota explicativa del proyecto de ley modelo sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza

I. Introducción

A. Finalidad de la presente Nota explicativa

1. Al preparar y adoptar la Ley Modelo de la CNUDMI sobre la Utilización y el Reconocimiento Transfronterizo de la Gestión de la Identidad y los Servicios de Confianza (en adelante, "la Ley Modelo"), la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) consideró que la Ley Modelo sería más eficaz para armonizar y modernizar la legislación si iba acompañada de información sobre sus antecedentes y explicaciones.

2. La presente Nota explicativa, que se basa en la labor preparatoria de la Ley Modelo, tiene por objeto ayudar a quienes tengan interés en la adopción, la utilización y la interpretación uniforme de la Ley Modelo, como los encargados de formular políticas, los legisladores, los académicos, los profesionales, los jueces y árbitros, los operadores comerciales y los usuarios de servicios de gestión de la identidad y servicios de confianza. Por ejemplo, en el momento de la incorporación al derecho interno, esa información podría ayudar a las distintas jurisdicciones a adaptar la Ley Modelo a sus necesidades en lo que respecta a la interacción entre las disposiciones de la Ley Modelo y el régimen regulador de la gestión de la identidad y los servicios de confianza.

B. Objetivos

3. En los últimos 20 años ha habido un crecimiento exponencial del valor de las actividades comerciales en línea (es decir, las operaciones electrónicas entre empresas, entre empresas y consumidores y entre empresas y Estados). Ese crecimiento, que se ha visto acelerado aún más por la necesidad de mitigar los efectos de la pandemia de COVID-19[1], ha venido acompañado de un aumento similar en las operaciones de datos y hace necesario adoptar un marco jurídico y técnico adecuado.

4. El crecimiento de las actividades comerciales en línea se basa en la confianza y tiene que ser respaldado por una sensación de confianza permanente en el entorno en línea. Un elemento importante de esa confianza es la capacidad de identificar de manera fiable a cada una de las partes, especialmente cuando no ha existido una interacción personal previa. La importancia de la identidad se reconoce en el Objetivo de Desarrollo Sostenible 16, cuya meta 9 es que se proporcione una identidad jurídica a todos los seres humanos, incluso en forma electrónica. En la economía digital, esto se traduce en el derecho a una identidad digital.

5. A lo largo de los años se han sugerido diversas soluciones para responder a la necesidad de identificación en línea. Como resultado de ello, se han concebido sistemas, métodos, tecnologías y dispositivos que se utilizan para crear y gestionar identidades digitales de personas físicas y jurídicas. El debate de los aspectos jurídicos de la gestión de la identidad a nivel mundial puede permitir no solo conciliar esas distintas soluciones, sino también fomentar la interoperabilidad entre los sistemas de gestión de la identidad, independientemente de que su funcionamiento esté a cargo de entidades públicas o privadas.

[1] UNCTAD, *Informe sobre la economía digital: Flujos de datos transfronterizos y desarrollo: Para quién fluyen los datos,* documento de las Naciones Unidas, UNCTAD/DER/2019, págs. 16 y 17.

6. Otro elemento importante de la confianza en línea es la posibilidad de confiar con seguridad suficiente en la calidad de los datos, que está en la base del intercambio de datos. Los servicios de confianza que ofrecen garantías sobre las propiedades de un mensaje de datos, como su origen, su integridad y el momento en que se procesa una determinada acción conexa, han surgido como soluciones para proporcionar esa confianza.

7. Los obstáculos que se oponen a una utilización más amplia de la gestión de la identidad y los servicios de confianza pueden ser de diversa índole. Por ejemplo, el acceso a la gestión de la identidad y los servicios de confianza puede verse limitado por el costo, la falta de información y las dificultades técnicas. Entre los obstáculos de carácter jurídico cabe citar los siguientes: 1) la falta de leyes que confieran efectos jurídicos a la gestión de la identidad y los servicios de confianza; 2) la divergencia de criterios jurídicos en materia de gestión de la identidad, en particular las leyes basadas en el uso de determinadas tecnologías; 3) la existencia de leyes que exigen el uso de documentos de identidad en papel para poder realizar operaciones comerciales en línea, y 4) la falta de mecanismos que permitan obtener el reconocimiento jurídico transfronterizo de la gestión de la identidad y los servicios de confianza[2].

8. El objetivo principal de la Ley Modelo es eliminar esos obstáculos mediante la elaboración de normas jurídicas uniformes que cumplen varios fines. Las normas uniformes pueden aumentar la eficiencia al promover la aceptación del resultado de la aplicación de la gestión de la identidad y los servicios de confianza en todos los ordenamientos; reducir los costos de transacción al facilitar el cumplimiento de los requisitos normativos; aumentar la previsibilidad y la seguridad jurídicas de las operaciones electrónicas sobre la base de un tratamiento común de las cuestiones, incluso con mecanismos de reconocimiento transfronterizo, y contribuir a cerrar la brecha digital facilitando la disponibilidad de soluciones comunes.

9. En particular, la creación de un marco jurídico para la gestión de la identidad y los servicios de confianza promoverá la implementación de la identidad digital y las operaciones de datos en condiciones de seguridad. Al fomentar la confianza en el entorno en línea, ese marco jurídico también contribuirá al desarrollo sostenible y a la inclusión social, en consonancia con el Objetivo de Desarrollo Sostenible 9, que se refiere a impulsar la innovación, entre otras cosas.

C. Ámbito de aplicación

10. La Ley Modelo es aplicable a la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza en el contexto de actividades comerciales y servicios relacionados con el comercio. Las jurisdicciones promulgantes pueden decidir ampliar el ámbito de aplicación de la Ley Modelo para que abarque actividades no comerciales.

11. Puede haber numerosas y diversas leyes que resulten pertinentes para el intercambio de datos. La Ley Modelo no tiene por objeto afectar a esas leyes ya existentes, es decir, al derecho aplicable a la protección y la privacidad de los datos. Tampoco introduce nuevas obligaciones de utilizar la gestión de la identidad o servicios de confianza, o un servicio de gestión de la identidad o un servicio de confianza en particular, ni afecta a ninguna obligación ya existente en tal sentido (véanse los párrs. 102 a 104 *infra*).

12. Las disposiciones de la Ley Modelo sobre la gestión de la identidad se aplican a la identificación de personas físicas y jurídicas. Las disposiciones relativas a los servicios de confianza se aplican a toda la información que exista en forma de mensaje de datos. Ambos grupos de disposiciones se aplican con independencia del carácter público o privado del proveedor de servicios, del usuario o de la parte que confía.

[2] A/CN.9/965, párr. 52.

D. Estructura

13. La Ley Modelo consta de cuatro capítulos, que tratan respectivamente de las disposiciones generales, la gestión de la identidad, los servicios de confianza y los aspectos internacionales. Los capítulos I y IV se aplican tanto a la gestión de la identidad como a los servicios de confianza. Además, la estructura y el contenido de los capítulos II y III guardan similitudes importantes. De ahí que la explicación de una disposición del capítulo II puede ser pertinente para la disposición correspondiente del capítulo III, en la medida en que las disposiciones coincidan. Ese puede ser el caso, en particular, de los artículos 13, 14, 15, 22, 23 y 24, en relación con los artículos 5; 6 y 7; 8; 10; 11 y 12, respectivamente.

14. El capítulo I contiene la definición de determinados términos utilizados en la Ley Modelo; la delimitación del ámbito de aplicación; disposiciones sobre la utilización voluntaria de la gestión de la identidad y los servicios de confianza, entre ellos algunos servicios determinados; disposiciones sobre la relación entre la Ley Modelo y otras leyes, incluidas las que imponen obligaciones de identificar o de utilizar servicios de confianza específicos, y disposiciones sobre la interpretación autónoma, en particular a los efectos de colmar lagunas, de la Ley Modelo a la luz de su carácter uniforme y su origen internacional.

15. En el capítulo II se establecen los elementos esenciales del régimen jurídico aplicable a la gestión de la identidad, se enuncian algunas obligaciones básicas de los proveedores de servicios de gestión de la identidad y de los usuarios, y se fijan normas relativas a la responsabilidad de los proveedores de servicios de gestión de la identidad. El artículo 5 consagra el principio del reconocimiento jurídico de la gestión de la identidad y de no discriminación contra la identificación electrónica. En el artículo 6 figura una lista de las obligaciones básicas de los proveedores de servicios de gestión de la identidad; de ese modo, se señalan las obligaciones fundamentales de los proveedores de servicios de gestión de la identidad, que corresponden a los elementos básicos de los sistemas de gestión de la identidad y a las principales etapas del ciclo de vida de la gestión de la identidad. El artículo 7 trata de las obligaciones de los proveedores de servicios de gestión de la identidad en caso de violación de los datos y se complementa con el artículo 8, relativo a las obligaciones de los usuarios en el caso de que las credenciales de identidad se vean comprometidas. El artículo 9 contiene una norma de equivalencia funcional entre la identificación fuera de línea y la identificación electrónica que exige la utilización de un método fiable. La fiabilidad del método se evalúa mediante una determinación *ex post* basada en las circunstancias indicadas en el artículo 10 o mediante una designación *ex ante* realizada con arreglo al artículo 11. Además, no es necesario determinar la fiabilidad del método si en la práctica este ha cumplido su función. Por último, el artículo 12 trata de la responsabilidad de los proveedores de servicios de gestión de la identidad.

16. En el capítulo III se establecen los elementos básicos del régimen jurídico aplicable a la utilización de los servicios de confianza. El artículo 13 contiene una norma general de no discriminación contra los efectos jurídicos de los servicios de confianza. El artículo 14 fija las obligaciones de los proveedores de servicios de confianza y el artículo 15 trata de las obligaciones de los usuarios de servicios de confianza en el caso de que el servicio se haya visto comprometido. En los artículos 16 a 21 se describen las funciones que se persiguen con determinados servicios de confianza previstos expresamente (firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, archivado electrónico, servicios de entrega electrónica certificada, autenticación de sitios web) y las obligaciones conexas, entre ellas la utilización de un método fiable. La mayoría de las disposiciones sobre los servicios de confianza previstos expresamente están redactadas como normas de equivalencia funcional. Sin embargo, dado que un servicio de confianza puede no tener un equivalente en papel, no requiere necesariamente una norma de equivalencia funcional. El artículo 22 sirve de orientación con respecto a la determinación *ex post* de la fiabilidad del método utilizado para el servicio de confianza y, el artículo 23, respecto de la designación *ex ante* de ese servicio.

Por último, el artículo 24 contiene normas sobre la responsabilidad de los proveedores de servicios de confianza.

17. El capítulo IV contiene normas que hacen posible el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza, que es uno de los principales objetivos de la Ley Modelo. La Ley Modelo no contempla la creación de un órgano dedicado específicamente al reconocimiento jurídico de la gestión de la identidad y los servicios de confianza, pero prevé varios mecanismos basados en un enfoque descentralizado. Además de los artículos 25, 26 y 27, son pertinentes las disposiciones dedicadas a esta cuestión que figuran en los artículos 10, párrafo 3; 11, párrafo 4; 22, párrafo 3, y 23, párrafo 4, que hacen referencia a la no discriminación por motivos geográficos a los efectos de determinar la fiabilidad de la gestión de la identidad y los servicios de confianza y designar sistemas de gestión de la identidad y servicios de confianza fiables. Los mecanismos contractuales también pueden ser importantes para permitir la utilización transfronteriza de la gestión de la identidad y los servicios de confianza.

E. Antecedentes

1. Proceso de redacción

18. La Ley Modelo tiene su origen en una solicitud formulada por la Comisión en su 48º período de sesiones, celebrado en 2015. En ese período de sesiones, la Comisión pidió a la secretaría que realizara una labor preparatoria sobre las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza, en particular organizando coloquios y reuniones de grupos de expertos, para que posteriormente la examinara un Grupo de Trabajo[3], y le solicitó también que informara al Grupo de Trabajo IV de los resultados de esa labor preparatoria con miras a obtener recomendaciones sobre el alcance exacto, la posible metodología y las prioridades, que se someterían a consideración de la Comisión[4].

19. En respuesta a esa solicitud, la Comisión, en su 49º período de sesiones, celebrado en 2016, tuvo ante sí una nota de la secretaría sobre los aspectos jurídicos relacionados con la gestión de la identidad y los servicios de confianza (A/CN.9/891) en la que se resumían las deliberaciones sostenidas durante el Coloquio de la CNUDMI sobre las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza, celebrado en Viena los días 21 y 22 de abril de 2016[5]. La Comisión convino en que el tema de la gestión de la identidad y los servicios de confianza siguiera figurando en el programa de trabajo del Grupo de Trabajo[6].

20. Tras recibir un mandato de la Comisión, el Grupo de Trabajo mantuvo deliberaciones preliminares sobre el tema en su 54º período de sesiones (Viena, 31 de octubre a 4 de noviembre de 2016). El Grupo de Trabajo acordó que su labor futura sobre la gestión de la identidad y los servicios de confianza se refiriera únicamente a la utilización con fines comerciales de sistemas de gestión de la identidad y que tuviera en cuenta a los proveedores de servicios de gestión de la identidad tanto públicos como privados. El Grupo de Trabajo convino también en que, si bien la labor relativa a la gestión de la identidad podría emprenderse antes que la labor sobre los servicios de confianza, los términos aplicables a ambos temas tendrían que determinarse y definirse simultáneamente, dada la estrecha relación existente entre ellos. Acordó asimismo que se prestara especial atención a los sistemas de gestión de la identidad pluripartitos y a la identificación de las personas físicas y jurídicas, y que el Grupo de Trabajo prosiguiera su labor aclarando en mayor medida los objetivos de la tarea propuesta,

[3] Documentos Oficiales de la Asamblea General, septuagésimo período de sesiones, suplemento núm. 17 (A/70/17), párrs. 354, 355 y 358.
[4] *Ibid.*, párr. 358.
[5] *Ibid.*, septuagésimo primer período de sesiones, suplemento núm. 17 (A/71/17), párr. 228.
[6] *Ibid.*, párrs. 235 y 236.

especificando su alcance, determinando los principios generales aplicables y redactando las definiciones necesarias (A/CN.9/897, párrs. 118 a 120 y 122).

21. En su 55º período de sesiones (Nueva York, 24 a 28 de abril de 2017), el Grupo de Trabajo, en consonancia con sus decisiones anteriores, analizó, entre otros asuntos, los objetivos, los principios generales y el alcance de su labor sobre la gestión de la identidad y los servicios de confianza (A/CN.9/902, párrs. 29 a 85).

22. La Comisión reafirmó el mandato que había otorgado al Grupo de Trabajo (véase el párr. 19 *supra*) en su 50º período de sesiones, celebrado en 2017, y pidió a la secretaría que estudiara la posibilidad de convocar reuniones de grupos de expertos. Se invitó a los Estados y las organizaciones internacionales a que transmitieran sus conocimientos especializados[7]. Así pues, la secretaría organizó una reunión de un grupo de expertos sobre los aspectos jurídicos de la gestión de la identidad y los servicios de confianza que se celebró en Viena los días 23 y 24 de noviembre de 2017.

23. También a la luz de las conclusiones de la reunión del grupo de expertos, en su 56º período de sesiones (Nueva York, 16 a 20 de abril de 2018) el Grupo de Trabajo señaló las cuestiones siguientes como pertinentes para su examen de los aspectos jurídicos de la gestión de la identidad y los servicios de confianza: alcance de la labor, principios generales, definiciones, requisitos y mecanismos para el reconocimiento recíproco, certificación de la gestión de la identidad y los servicios de confianza, niveles de garantía con respecto a la gestión de la identidad y los servicios de confianza, responsabilidad, mecanismos de cooperación institucional, transparencia, obligación de identificar, conservación de los datos, y supervisión de los proveedores de servicios (A/CN.9/936, párrs. 61 a 94).

24. Por recomendación del Grupo de Trabajo (A/CN.9/936, párr. 95), la Comisión, en su 51er período de sesiones, celebrado en 2018, solicitó al Grupo de Trabajo que emprendiera una labor con miras a preparar un texto destinado a facilitar el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza, sobre la base de los principios y cuestiones señalados por el Grupo de Trabajo (véase el párr. 23 *supra*)[8].

25. En consecuencia, el Grupo de Trabajo continuó examinando las cuestiones que había señalado (A/CN.9/965, párrs. 10 a 129) en su 57º período de sesiones (Viena, 19 a 23 de noviembre de 2018).

26. En el 58º período de sesiones del Grupo de Trabajo (Nueva York, 8 a 12 de abril de 2019), se sometió a consideración de este un primer proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza (A/CN.9/WG.IV/WP.157), acompañado de observaciones explicativas (A/CN.9/WG.IV/WP.158). El Grupo de Trabajo examinó las disposiciones del proyecto que se referían al ámbito de aplicación, el reconocimiento y la fiabilidad de los sistemas de gestión de la identidad y los servicios de confianza, los tipos de servicios de confianza que estarían comprendidos y las obligaciones y la responsabilidad de los proveedores de servicios de gestión de la identidad y de servicios de confianza (A/CN.9/971, párrs. 13 a 153).

27. En ese período de sesiones, el Grupo de Trabajo pidió a la secretaría que preparara, en consulta con expertos, propuestas concretas sobre cuestiones relativas a la fiabilidad de los sistemas de gestión de la identidad (A/CN.9/971, párr. 67). En atención a esa solicitud, la secretaría convocó una reunión de un grupo de expertos, que se celebró en Viena los días 22 y 23 de julio de 2019, a fin de examinar las normas y procedimientos a que debían ajustarse los sistemas de gestión de la identidad a efectos de su reconocimiento jurídico, así como otras cuestiones contempladas en el proyecto de disposiciones, en particular, la fiabilidad de esos sistemas y las obligaciones y la responsabilidad de los proveedores de servicios de gestión de la identidad.

[7] *Ibid.*, septuagésimo segundo período de sesiones, suplemento núm. 17 (A/72/17), párr. 127.
[8] *Ibid.*, septuagésimo tercer período de sesiones, suplemento núm. 17 (A/73/17), párr. 159.

28. La Comisión expresó su satisfacción por los progresos realizados por el Grupo de Trabajo en su 52º período de sesiones, celebrado en 2019[9]. Señaló que la labor del Grupo de Trabajo debía encaminarse a elaborar un instrumento que pudiera aplicarse a la utilización de la gestión de la identidad y los servicios de confianza tanto a nivel nacional como a través de fronteras, y que el resultado de la labor repercutiría en aspectos que iban más allá de las operaciones comerciales[10].

29. En su 59º período de sesiones (Viena, 25 a 29 de noviembre de 2019), el Grupo de Trabajo examinó una versión revisada del proyecto de disposiciones (A/CN.9/WG.IV/WP.160) en la que se tenían en cuenta los resultados de las consultas mantenidas por la secretaría con expertos (véase el párr. 27 *supra*). El Grupo de Trabajo procedió a una lectura completa del proyecto, centrándose en las disposiciones relativas a los servicios de confianza (A/CN.9/1005, párrs. 10 a 122). También sostuvo deliberaciones preliminares sobre la forma del instrumento, y se expresó una preferencia clara por que este adoptara la forma de una ley modelo, en lugar de una convención (*ibid*., párr. 123).

30. La Comisión expresó nuevamente su satisfacción por los progresos realizados por el Grupo de Trabajo en su 53er período de sesiones, celebrado en 2020[11].

31. El Grupo de Trabajo tuvo ante sí una segunda versión revisada del proyecto de disposiciones (A/CN.9/WG.IV/WP.162) y realizó una lectura completa de esas disposiciones (A/CN.9/1045, párrs. 16 a 138) en su 60º período de sesiones (Viena, 19 a 23 de octubre de 2020). También estuvo de acuerdo con la posibilidad de celebrar consultas oficiosas a fin de debatir las cuestiones pendientes.

32. Del 15 al 17 de marzo de 2021 se celebraron consultas oficiosas a distancia con delegados y observadores para tratar los temas de la responsabilidad, la relación entre el proyecto de disposiciones y los textos vigentes de la CNUDMI, el reconocimiento transfronterizo, y las definiciones y otras cuestiones terminológicas.

33. El Grupo de Trabajo recibió información sobre los resultados de las consultas oficiosas en su 61er período de sesiones (Nueva York, 6 a 9 de abril de 2021). En vista de las limitaciones derivadas del formato híbrido del período de sesiones (entre ellas la menor duración de las reuniones), al examinar una tercera versión revisada del proyecto de disposiciones (A/CN.9/WG.IV/WP.167) el Grupo de Trabajo centró sus deliberaciones en las cuestiones analizadas durante las consultas (A/CN.9/1051, párrs. 13 a 67).

34. Se informó a la Comisión, en su 54º período de sesiones, celebrado en 2021, que pese a la menor duración de las reuniones el Grupo de Trabajo había avanzado considerablemente hacia la finalización del instrumento. La Comisión expresó su satisfacción y alentó al Grupo de Trabajo a que finalizara su labor y se la presentara para examinarla en su 55º período de sesiones, en 2022[12].

35. En su 62º período de sesiones (Viena, 22 a 26 de noviembre de 2021), el Grupo de Trabajo realizó una nueva lectura del proyecto de disposiciones (A/CN.9/1087, párrs. 12 a 114) sobre la base de una versión revisada (A/CN.9/WG.IV/WP.170) acompañada de una nota explicativa (A/CN.9/WG.IV/WP.171). El Grupo de Trabajo solicitó a la secretaría que revisara el proyecto de disposiciones y la nota explicativa para que reflejaran sus deliberaciones y decisiones y que remitiera el texto revisado a la Comisión, en forma de ley modelo, para que esta lo examinara en su 55º período de sesiones. Se pidió a la secretaría que transmitiera el texto revisado a todos los Gobiernos y organizaciones internacionales pertinentes para que formularan observaciones, y que recopilara las observaciones recibidas a fin de someterlas a consideración de la Comisión (A/CN.9/1087, párr. 11).

[9] *Ibid.*, septuagésimo cuarto período de sesiones, suplemento núm. 17 (A/74/17), párr. 175.
[10] *Ibid.*, párr. 172.
[11] *Ibid.*, septuagésimo quinto período de sesiones, suplemento núm. 17 (A/75/17), segunda parte, párrs. 41 y 51 d).
[12] *Ibid.*, septuagésimo sexto período de sesiones, suplemento núm. 17 (A/76/17), cap. IX.

36. [Se completará.]

2. Relación con textos anteriores de la CNUDMI

37. No existe ninguna disposición sobre los servicios de confianza en los textos anteriores de la CNUDMI. Sin embargo, esos textos enuncian normas de equivalencia funcional que pueden ser pertinentes para determinados servicios de confianza. El artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico ("LMCE")[13], el artículo 6 de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas ("LMFE")[14], el artículo 9, párrafo 3, de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales ("CCE")[15] y el artículo 9 de la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos ("LMDTE")[16] establecen los requisitos que deben reunir las firmas electrónicas para ser equivalentes funcionales de las firmas en papel. En esas disposiciones se exige la identificación del firmante, lo que puede implicar el uso de la identificación electrónica y, más en general, de la gestión de la identidad. El artículo 16 de la Ley Modelo se basa en el artículo 9 de la LMDTE.

38. De manera similar, el artículo 10 de la LMCE establece los requisitos para la equivalencia funcional de la conservación de información, y el artículo 19 de la Ley Modelo se basa en el artículo 10, párrafo 1, de la LMCE. Otras disposiciones de la CNUDMI que se han utilizado como fuentes de los artículos de la Ley Modelo se indican en el comentario del artículo respectivo. Sin embargo, es posible que no sea necesario utilizar alguno de los servicios de confianza previstos expresamente en la Ley Modelo para cumplir las normas de equivalencia funcional establecidas en textos anteriores de la CNUDMI.

39. Varias cuestiones importantes para la Ley Modelo, como la evaluación de la fiabilidad, la responsabilidad y los mecanismos de reconocimiento transfronterizo, se han analizado en detalle en un documento de orientación sobre el uso de la firma electrónica en el plano internacional[17].

F. Conceptos y principios fundamentales

40. En esta sección se explican varios de los conceptos y principios fundamentales en los que se basa la Ley Modelo. En el comentario del artículo 1 que figura más abajo se explican en mayor detalle los términos definidos empleados en la Ley Modelo, y en el documento A/CN.9/WG.IV/WP.150 se puede consultar una lista más extensa de términos y conceptos relacionados con la gestión de la identidad y los servicios de confianza recopilados a partir de las definiciones enunciadas en textos jurídicos y técnicos convenidos internacionalmente. Como se señala en ese documento, es posible que en esos textos se empleen términos definidos diferentes para hacer referencia al mismo concepto o que se defina el mismo término de distinta manera.

---

[13] CNUDMI, *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno, 1996, con el nuevo artículo 5 bis aprobado en 1998* (1999), publicación de las Naciones Unidas, núm. de venta: S.99.V.4.

[14] CNUDMI, *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno* (2002), publicación de las Naciones Unidas, núm. de venta: S.02.V.8.

[15] Naciones Unidas, *Treaty Series*, vol. 2898, pág. 3.

[16] CNUDMI, *Ley Modelo sobre Documentos Transmisibles Electrónicos* (2018), publicación de las Naciones Unidas, núm. de venta: S.17.V.5.

[17] Secretaría de la CNUDMI, *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas* (2007), publicación de las Naciones Unidas, núm. de venta S.09.V.4.

1. Principios fundamentales

41. Al igual que textos anteriores de la CNUDMI, la Ley Modelo se basa en los principios de autonomía de las partes, neutralidad tecnológica, equivalencia funcional y no discriminación contra la utilización de medios electrónicos, con adaptaciones[18].

42. El principio de autonomía de las partes permite a las partes contratantes elegir las reglas aplicables, dentro de los límites impuestos por las normas jurídicas imperativas. Se basa en el reconocimiento de que las partes pueden ser quienes estén en mejores condiciones para determinar cuáles son las reglas más adecuadas para la operación de que se trate.

43. El principio de no discriminación, formulado por primera vez en el artículo 5 de la LMCE y conocido también como principio del reconocimiento jurídico, propugna que no se nieguen efectos jurídicos, validez ni fuerza ejecutoria a la información por la sola razón de que esté en forma electrónica.

44. El principio de neutralidad tecnológica aboga por que la ley no imponga ni favorezca el uso de ninguna tecnología o método en particular y, de ese modo, evita que las leyes se vuelvan obsoletas con el tiempo. La neutralidad tecnológica es necesaria para lograr la interoperabilidad, que permite efectivamente la circulación de datos. El fundamento jurídico de este principio es la definición amplia de “mensaje de datos”, enunciada por primera vez en el artículo 2 a) de la LMCE, que pretende abarcar todas las tecnologías existentes y futuras.

45. El principio de equivalencia funcional establece los criterios según los cuales se considera que las operaciones electrónicas cumplen los requisitos de forma aplicables a los documentos en papel, por ejemplo, que un documento debe constar por escrito, ser original o estar firmado. Presupone la existencia de requisitos legales que directa o indirectamente exigen alguna actividad física o en papel, como la utilización de una credencial emitida en papel para identificar a una persona. Además, analiza los fines y las funciones de esos requisitos con vistas a determinar cómo se podrían cumplir esos fines o funciones por medios electrónicos.

46. Si bien esos principios generales no se mencionan expresamente en la Ley Modelo, en ellos se enmarcan las disposiciones fundamentales del texto. El principio de autonomía de las partes se recoge en el artículo 3, y el principio de no discriminación, tal como se aplica a la gestión de la identidad y a los servicios de confianza, está consagrado en los artículos 5 y 13, respectivamente. Además, el principio de equivalencia funcional ha inspirado el artículo 9, sobre la identificación electrónica, y los artículos 16 a 21, que tratan de los servicios de confianza previstos expresamente. No obstante, es posible que algunos de los servicios de confianza contemplados en la Ley Modelo no tengan un equivalente en papel y, por consiguiente, no se les aplicaría el principio de equivalencia funcional.

2. Gestión de la identidad

47. La identificación es el proceso por el cual se distingue a una persona de otra sobre la base de la información relativa a esa persona (es decir, sus atributos). Esa información puede recopilarse u observarse. La identificación conlleva verificar que los atributos recopilados u observados corresponden a una “identidad” establecida anteriormente respecto de la persona que se quiere identificar. La identificación en ese sentido suele realizarse en respuesta a una persona que alega tener determinada identidad y presenta atributos para que se verifique esa identidad.

[18] A/CN.9/902, párrs. 52 y 63.

48. En consecuencia, según la Ley Modelo, la gestión de la identidad comprende dos etapas (o fases) claramente diferenciadas: en primer lugar, la emisión de las credenciales de identidad, es decir, datos que pueden presentarse para la identificación electrónica, y, en segundo lugar, la presentación y verificación de esas credenciales por medios electrónicos:

a) La primera etapa de la gestión de la identidad consiste en recopilar los atributos que pueden constituir la "identidad básica" de la persona (es decir, atributos que son registrados por organismos públicos en sistemas de registro civil y estadísticas vitales en el caso de las personas físicas y en registros de sociedades o empresas en el caso de las personas jurídicas). Esos atributos pueden presentarse en forma de credenciales emitidas por el Estado (p. ej., un certificado de inscripción) y verificadas por el organismo emisor. Ese proceso, que puede llevarse a cabo "fuera de línea" a partir de las credenciales físicas presentadas en persona, tiene como resultado la emisión de credenciales a la persona en cuestión;

b) La segunda etapa de la gestión de la identidad consiste en presentar esas credenciales por medios electrónicos y verificar por medios electrónicos que la persona cuyas credenciales se presentan es la persona a quien se emitieron las credenciales en la primera etapa.

49. Los sistemas de gestión de la identidad se utilizan para gestionar los procesos de identificación asociados a cada una de las dos etapas, así como para gestionar los atributos recopilados, las credenciales emitidas y los medios de verificación empleados. Los sistemas de gestión de la identidad pueden suponer la existencia de una sola entidad que ejecuta todos los procesos que integran cada una de las etapas de la gestión de la identidad, o de varias entidades que ejecutan esos procesos. Además, un sistema de gestión de la identidad puede ofrecer diferentes servicios de gestión de la identidad. Las partes (es decir, la parte que quiere identificar y la parte que quiere ser identificada) pueden elegir el servicio de gestión de la identidad que consideren más adecuado en función de sus necesidades.

50. Los sistemas de gestión de la identidad pueden ser operados por entidades públicas o privadas. En la práctica, los sistemas públicos corresponden por lo general a un solo servicio de gestión de la identidad, mientras que los sistemas privados pueden corresponder a múltiples servicios de gestión de la identidad con distintos niveles de fiabilidad. Otra clasificación de los sistemas de gestión de la identidad responde a su carácter centralizado o distribuido. En aplicación del principio de neutralidad tecnológica (véase el párr. 44 *supra*), la Ley Modelo no presupone la utilización de ninguna tecnología o modelo, por lo que puede aplicarse a todos los tipos de sistemas y servicios de gestión de la identidad.

51. Los proveedores de servicios de gestión de la identidad, los usuarios, las partes que confían y otras entidades interesadas pueden convenir en regirse por políticas, normas y tecnologías compatibles, que se especifican en las normas del sistema, de modo que todas las partes intervinientes que confían puedan entender las credenciales proporcionadas por los distintos proveedores de servicios de gestión de la identidad intervinientes y confiar en ellas. Se puede aludir a ese mecanismo con el nombre de "sistema federado de identidad", y las normas del sistema, que son de carácter contractual, pueden denominarse "marco de confianza". Los sistemas federados de identidad pueden contribuir a aumentar el número de usuarios y de aplicaciones que comparten los mismos servicios de gestión de la identidad, lo cual, a su vez, puede reducir los costos y, de ese modo, lograr la sostenibilidad a largo plazo.

3. Servicios de confianza

52. Los servicios de confianza son servicios en línea que ofrecen garantías respecto de determinadas propiedades de los mensajes de datos, como la fuente, la integridad y el momento en que se procesó determinada acción con respecto a los datos. Garantizar la calidad de los datos es fundamental para establecer la confianza en las actividades de intercambio de datos, que son la columna vertebral del comercio digital. En la Ley Modelo se señalan determinados servicios de confianza que se utilizan habitualmente y

se reconoce la posibilidad de que existan o se desarrollen otros servicios de confianza en el futuro.

53. El concepto de servicio de confianza recogido en la Ley Modelo se refiere a la prestación de un servicio y no simplemente al servicio en sí mismo. Por ejemplo, una firma electrónica puede estamparse mediante un servicio que utiliza métodos para crear y gestionar una firma electrónica. A fin de disipar dudas, en cada una de las disposiciones de la Ley Modelo se especifica si la disposición se refiere a los métodos utilizados para la prestación del servicio de firma electrónica, o a la firma electrónica resultante de la utilización de ese servicio.

4. Evaluación de la fiabilidad

54. En consonancia con textos anteriores de la CNUDMI, varias disposiciones de la Ley Modelo hacen referencia a la utilización de un método fiable para la prestación de servicios de gestión de la identidad y servicios de confianza. La Ley Modelo prevé dos mecanismos para evaluar la fiabilidad del método: en los artículos 10 y 22 figura una lista indicativa de factores pertinentes para determinar la fiabilidad, y en los artículos 11 y 23 se establece un mecanismo para designar métodos fiables.

a) Designación *ex ante* de la fiabilidad

55. Un criterio posible para evaluar la fiabilidad de un método es exigir que la evaluación se lleve a cabo antes de que se utilice el método ("*ex ante*"), en función de una lista de condiciones predeterminadas y con carácter general, no en relación con una operación en particular. En la Ley Modelo se hace referencia a este criterio como designación de la fiabilidad y se enuncian, en el artículo 11 (aplicable a los servicios de gestión de la identidad) y en el artículo 23 (aplicable a los servicios de confianza), los requisitos para la designación, entre los que se incluyen las mismas circunstancias que se tienen en cuenta para la determinación de la fiabilidad.

56. El objeto de la designación no es una categoría genérica de servicios de gestión de la identidad o de servicios de confianza, ni todos los servicios de gestión de la identidad o todos los servicios de confianza ofrecidos por un proveedor de esos servicios, sino más bien un servicio concreto prestado por un determinado proveedor de servicios.

57. El criterio *ex ante* puede ofrecer un mayor grado de claridad y previsibilidad que el criterio *ex post* en cuanto a los efectos jurídicos de la gestión de la identidad y los servicios de confianza, en particular cuando se utilizan a través de fronteras. Sin embargo, la gobernanza en este aspecto presupone la existencia de un mecanismo institucional, es decir, una entidad que sea competente para administrar el proceso de designación.

58. La jurisdicción promulgante que desee aplicar el criterio *ex ante* debe indicar cuál será la entidad encargada de la designación, que puede ser un organismo público o privado. Las entidades designadoras pueden obtener su acreditación con arreglo a las normas técnicas aplicables a los organismos que certifican productos, procesos o servicios. La certificación (incluida la autocertificación) es útil para evaluar los servicios aplicando normas basadas en los resultados y, por lo tanto, puede ser pertinente para la designación de los servicios.

59. La Ley Modelo presupone la existencia del mecanismo institucional necesario para aplicar el criterio *ex ante*, pero no prevé su establecimiento o administración. Ese mecanismo tendrá que incluir diversos elementos, como criterios para evaluar los servicios, detalles sobre el proceso de evaluación para la adopción de decisiones, y fuentes de financiación. La gobernanza de ese sistema de otorgamiento de licencias puede ser compleja y costosa, dependiendo de varios factores, entre ellos los mecanismos institucionales. Por ese motivo, puede ser preferible aplicar la designación a los servicios que ofrezcan niveles más altos de garantía y fiabilidad y que, por ende, sean utilizados para operaciones de mayor valor.

60. El mecanismo de designación debería adaptarse rápidamente a la evolución tecnológica para no poner obstáculos a la innovación. De lo contrario, podría discriminar a los servicios de gestión de la identidad y los servicios de confianza que, pese a estar disponibles y basarse en métodos fiables, no hubieran sido designados. Además, una mayor especificación de las condiciones exigidas para la designación no debería traducirse en la imposición de la obligación de utilizar determinadas tecnologías.

b) Determinación *ex post* de la fiabilidad

61. Otro criterio posible para evaluar la fiabilidad de un método consiste en posponer la evaluación hasta el momento en que surja una controversia sobre la fiabilidad. En consecuencia, la evaluación se lleva a cabo solo después de utilizado el método ("*ex post*"). En la Ley Modelo se hace referencia a este criterio como determinación de la fiabilidad y se enuncian, en el artículo 10 (aplicable a los servicios de gestión de la identidad) y en el artículo 22 (aplicable a los servicios de confianza), los requisitos exigidos para esa determinación, entre ellos una lista no taxativa de circunstancias pertinentes.

62. Por lo general, el criterio *ex post* permite que las operaciones de gestión de la identidad se lleven a cabo sin una evaluación previa de la fiabilidad y solo exige que se evalúe la fiabilidad en los casos en que efectivamente se plantea una controversia. También ofrece la máxima flexibilidad a las partes en la elección de tecnologías y métodos. Además, puede administrarse de manera descentralizada y no obliga a establecer un mecanismo institucional, evitando así los gastos que ello supondría.

63. Por otro lado, es posible que el criterio *ex post* no ofrezca un mayor grado de previsibilidad en cuanto a la validez del método empleado antes de que este se utilice efectivamente, exponiendo así a las partes al riesgo de que el método no llegue a considerarse fiable. Además, deja la determinación de la fiabilidad del método en manos de un tercero que dirime la cuestión mediante un proceso que puede ser prolongado y dar lugar a decisiones incongruentes.

c) Criterio mixto

64. La Ley Modelo combina la determinación con la designación, permitiendo así el reconocimiento de cualquier servicio de gestión de la identidad y cualquier servicio de confianza y, al mismo tiempo, proporcionando orientación sobre qué servicios de gestión de la identidad y qué servicios de confianza ofrecen un mayor grado de confianza en su fiabilidad (criterio "dual"). De ese modo, la Ley Modelo no favorece un mecanismo en detrimento del otro, sino que procura combinar las ventajas de ambos mecanismos, a la vez de reducir al mínimo sus inconvenientes, y, en última instancia, permite que se aplique la solución que prefieran las partes.

65. No todos los textos de la CNUDMI contienen disposiciones que incorporen tanto el criterio *ex ante* como el criterio *ex post*. Sin embargo, estos dos criterios suelen considerarse compatibles y complementarios. El criterio mixto adoptado en la Ley Modelo se basa en los artículos 6 y 7 de la LMFE.

5. Cuestiones de responsabilidad

66. El régimen de responsabilidad puede influir de manera considerable en el fomento de la utilización de la gestión de la identidad y los servicios de confianza y es un elemento fundamental de la Ley Modelo. Históricamente, los legisladores han adoptado distintas soluciones, desde no establecer un régimen de responsabilidad específico hasta aprobar disposiciones sobre normas de conducta y reglas de responsabilidad aplicables únicamente a los proveedores de servicios, o a todas las partes interesadas (proveedores

de servicios, usuarios y partes que confían)[19]. Este último criterio fue el que se adoptó en la LMFE[20].

67. La responsabilidad relativa a los servicios de gestión de la identidad y los servicios de confianza se asigna principalmente mediante acuerdos contractuales o por disposición de la ley. Puede ser preferible adoptar este último criterio para evitar que puedan excluirse determinadas disposiciones por la vía del contrato. Además, las normas legales pueden aplicarse también cuando no existe un acuerdo contractual, es decir, con respecto a las partes que confían.

68. En los artículos 12 y 24 se establece un régimen de responsabilidad uniforme de los proveedores de servicios frente a los usuarios y las partes que confían, basado en el principio de que todo proveedor de servicios debe responder de las consecuencias del incumplimiento de su obligación de prestar los servicios en la forma exigida por la ley. Por consiguiente, los artículos 12 y 24 establecen un fundamento legal de la responsabilidad que se aplica junto con la responsabilidad contractual y extracontractual. Además, la Ley Modelo permite a los proveedores de servicios limitar su responsabilidad tanto frente a los usuarios como frente a las partes que confían.

69. La Ley Modelo no se refiere ni al grado de culpa necesario para incurrir en responsabilidad ni al tipo de daños resarcibles y su cuantía[21]. Por lo tanto, las normas del derecho ordinario de la jurisdicción promulgante serían aplicables a esas cuestiones si en el momento de la incorporación de la Ley Modelo al derecho interno no se adoptara ninguna norma especial aplicable a los proveedores de servicios de gestión de la identidad y servicios de confianza.

6. Aspectos internacionales

70. La dimensión internacional es esencial para la utilización de la gestión de la identidad y los servicios de confianza y, en general, de las operaciones electrónicas. Sin embargo, hay dos tipos de obstáculos que pueden dificultar esa utilización: la incompatibilidad técnica que da lugar a la falta de interoperabilidad y los obstáculos jurídicos para el reconocimiento transfronterizo[22].

71. Los obstáculos jurídicos pueden derivarse de la existencia de criterios nacionales contradictorios, especialmente cuando la ley impone o favorece una tecnología, un método o un producto determinados. En ese caso, los requisitos legales nacionales pueden impedir el reconocimiento de los tipos de servicios de gestión de la identidad o de confianza que no se ajusten a ellos. Además, el surgimiento de normas técnicas nacionales —que también puede producirse en el marco del criterio “dual”, cuando esas normas están vinculadas a presunciones legales— puede dar lugar a un mosaico de requisitos que también tiene el efecto de obstaculizar el uso a través de fronteras.

72. Uno de los principales objetivos de la Ley Modelo es hacer posible legalmente la utilización transfronteriza de la gestión de la identidad y los servicios de confianza. Ello se logra mediante la aplicación de los principios de neutralidad tecnológica y no discriminación por razón del origen geográfico[23], que se recogen en los artículos 10, párrafo 3; 11, párrafo 4; 22, párrafo 3, y 23, párrafo 4, de la Ley Modelo. Además, el capítulo IV trata concretamente de los asuntos relacionados con el reconocimiento transfronterizo. En consecuencia, la Ley Modelo no solo desalienta la aprobación de leyes basadas en el uso de una tecnología en particular, sino que además fomenta la

[19] *Fomento de la confianza en el comercio electrónico*, párr. 175.

[20] Para más detalles véase la *Nota explicativa* de la LMFE, párrs. 77 a 81.

[21] Sobre estas cuestiones, véase *Fomento de la confianza en el comercio electrónico*, párrs. 177 a 193 (fundamento de la responsabilidad: negligencia o culpa simple, negligencia presunta y responsabilidad objetiva) y párrs. 194 a 201 (partes con derecho a reclamar daños y perjuicios y magnitud de los daños resarcibles).

[22] *Fomento de la confianza en el comercio electrónico*, párrs. 137 a 152.

[23] La neutralidad tecnológica y un enfoque no discriminatorio respecto de las firmas y servicios extranjeros ya habían sido señalados como principios que sustentan el consenso que está surgiendo en torno a los mecanismos jurídicos de reconocimiento transfronterizo de las firmas electrónicas en el documento titulado *Fomento de la confianza en el comercio electrónico*, párr. 149.

elaboración de normas técnicas interoperables, entre otras cosas mediante la cooperación.

73. La Ley Modelo, en consonancia con el criterio adoptado en textos anteriores de la CNUDMI, va más allá de la mera referencia al lugar de origen como factor pertinente para conceder el reconocimiento jurídico a servicios de gestión de la identidad y servicios de confianza extranjeros. Más concretamente, exige la determinación *ex post* de la fiabilidad de los servicios de gestión de la identidad y servicios de confianza extranjeros sobre la base de las mismas circunstancias que deben tenerse en cuenta para servicios nacionales análogos. También prevé mecanismos para la designación de la fiabilidad de los servicios de gestión de la identidad y servicios de confianza extranjeros sobre la base de las mismas circunstancias que deben tenerse en cuenta para servicios nacionales análogos. En síntesis, debería ser la fiabilidad técnica, y no el lugar de origen, el factor que determine si corresponde otorgar el reconocimiento jurídico.

74. La Ley Modelo no exige que se establezca un mecanismo institucional oficial para el reconocimiento jurídico transfronterizo. Sin embargo, hay ejemplos de ese tipo de mecanismos en los planos regional y bilateral. Las jurisdicciones promulgantes tal vez deseen utilizar la Ley Modelo como marco de referencia para establecer un mecanismo institucional con asociados internacionales, por ejemplo mediante la celebración de un acuerdo específico con ese fin.

75. Los capítulos sobre comercio electrónico que figuran en los acuerdos de libre comercio suelen contener disposiciones sobre la firma electrónica u otras formas de identificación electrónica, a menudo denominadas “métodos de autenticación”, y exigen cada vez más el reconocimiento recíproco de los métodos de identificación electrónica. Además, los acuerdos sobre la economía digital tienen un módulo dedicado a la identidad digital cuyo fin es hacer posible la interoperabilidad transfronteriza. La incorporación de la Ley Modelo al derecho interno puede contribuir a la aplicación de esas disposiciones de los acuerdos de libre comercio y los acuerdos sobre la economía digital.

II. Comentario artículo por artículo

A. Capítulo I. Disposiciones generales (artículos 1 a 4)

1. Artículo 1. Definiciones

76. El artículo 1 contiene las definiciones de los términos utilizados en la Ley Modelo.

“Atributo”

77. Por “atributo” se entenderá un elemento de información o datos relacionados con una persona. Son ejemplos de atributos de una persona física el nombre, la dirección, la edad y la dirección electrónica, y también datos como la presencia en la red y el dispositivo utilizado. Son ejemplos de atributos de una persona jurídica la razón social, la dirección de la oficina principal, el nombre con el que figura en el registro y la jurisdicción en la que está inscrita. El concepto de atributo se utiliza en la definición de identidad.

78. Los atributos pueden contener datos personales que se rigen por las leyes de protección y privacidad de los datos. La Ley Modelo no regula la protección y la privacidad de los datos y preserva expresamente la aplicación de esas leyes.

Referencias

A/CN.9/WG.IV/WP.150, párr. 13.

“Mensaje de datos”

79. La definición de “mensaje de datos” puede encontrarse en todos los textos vigentes de la CNUDMI sobre comercio electrónico, en los que se utiliza para aplicar el principio de neutralidad tecnológica (véase el párr. 44 *supra*). Este término es el principal punto de referencia para definir los requisitos que deben reunir los servicios de confianza, ya que el resultado de la aplicación de un servicio de confianza es la garantía de las propiedades de un mensaje de datos.

Referencias

A/CN.9/1045, párr. 40.

“Identificación electrónica” [“Autenticación”]

80. El término “identificación electrónica” se refiere a la verificación del vínculo existente entre la supuesta identidad de una persona física o jurídica y las credenciales presentadas, que es la segunda etapa de la gestión de la identidad. Se utiliza el término “identificación electrónica” en lugar del término “autenticación” debido a las preocupaciones expresadas con respecto a los múltiples significados que se atribuyen al término “autenticación”. En el uso técnico, el término “autenticación” se refiere a la presentación de pruebas de la identidad.

81. Es posible que no sea necesario revelar el nombre de la persona física o jurídica para cumplir los requisitos de identificación electrónica cuando baste con verificar otros atributos. Esto está en consonancia con el criterio adoptado en textos anteriores de la CNUDMI, en particular la LMFE, según la cual “a efectos de definición de la ‘firma electrónica’ en la Ley Modelo, el concepto de ‘identificación’ podría ser más que la mera identificación del firmante por su nombre”[24].

82. El término “identificación” sin calificación alguna se utiliza en un sentido no técnico en el artículo 9.

Referencias

A/CN.9/1005, párrs. 13, 84 a 86 y 92; A/CN.9/1045, párrs. 134 y 136; A/CN.9/1051, párr. 67.

“Identidad”

83. La definición de “identidad” está en el núcleo del concepto de gestión de la identidad y se refiere a la capacidad de distinguir de manera inequívoca a una persona física o jurídica en un contexto determinado. Es, por tanto, un concepto que depende del contexto. Esta definición se extrajo de la que figura en la Recomendación UIT-T X.1252, cláusula 6.40.

Referencias

A/CN.9/WG.IV/WP.150, párr. 31; A/CN.9/1005, párr. 108.

“Credenciales de identidad”

84. Las “credenciales de identidad” son los datos, o el objeto físico que contiene los datos, que se presentan a los efectos de la comprobación de la identidad. Son ejemplos de credenciales digitales los nombres de usuario, las tarjetas inteligentes, los certificados digitales y de identidad móviles, los pasaportes biométricos y las tarjetas de identidad electrónicas. Las credenciales de identidad en forma electrónica pueden utilizarse en línea o fuera de línea según las características del sistema de gestión de la identidad. El término “credenciales de identidad” es, en términos generales, sinónimo

[24] LMFE, *Nota explicativa*, párr. 117.

del término “medios de identificación electrónica” que se utiliza en la legislación regional y nacional (p. ej., en el Reglamento eIDAS, art. 3, párr. 2)[25].

Referencias

A/CN.9/1005, párr. 110; A/CN.9/1045, párr. 137.

“Servicios de gestión de la identidad”

85. La definición de “servicios de gestión de la identidad” refleja el entendimiento de que la gestión de la identidad comprende dos etapas (o fases): la “comprobación de la identidad” y la “identificación electrónica”. La definición de servicios de gestión de la identidad se refiere a los servicios que guardan relación con cualquiera de esas dos etapas o con ambas, ya que el uso de la palabra “o” en esa definición no es disyuntivo. En el artículo 6 a), que trata de las obligaciones básicas de los proveedores de servicios de gestión de la identidad, se describen las diversas etapas y pasos que comprende la prestación de servicios de gestión de la identidad.

Referencias

A/CN.9/1005, párrs. 84 y 109; A/CN.9/1087, párr. 19.

“Proveedor de servicios de gestión de la identidad”

86. El proveedor de servicios de gestión de la identidad es la persona física o jurídica que presta servicios de gestión de la identidad desempeñando, directamente o por intermedio de subcontratistas, las funciones indicadas en el artículo 6. Sin embargo, es posible que no todas las funciones mencionadas en ese artículo sean aplicables a todos los sistemas de gestión de la identidad y, por consiguiente, un proveedor de servicios de gestión de la identidad no desempeñará necesariamente todas y cada una de las funciones allí indicadas. La mención de la existencia de un acuerdo con el usuario es un recordatorio de que el proveedor de servicios de gestión de la identidad es responsable de todo el conjunto de servicios prestados, independientemente de que las funciones conexas sean cumplidas directamente, o por terceros en calidad de contratistas.

Referencias

A/CN.9/971, párr. 97; A/CN.9/1005, párr. 111; A/CN.9/1045, párr. 88; A/CN.9/1087, párr. 22.

“Sistema de gestión de la identidad”

87. La definición de “sistema de gestión de la identidad” describe el sistema utilizado para gestionar la identidad mediante la comprobación de la identidad y la identificación electrónica. Hace referencia a las “funciones y capacidades”, de acuerdo con la terminología de la UIT, a saber, la Recomendación UIT-T X.1252, cláusula 6.43. A diferencia de la definición de “servicios de gestión de la identidad”, la definición de “sistema de gestión de la identidad” comprende necesariamente ambas etapas, incluso en el caso de que intervengan distintos proveedores de servicios en cada una de ellas.

Referencias

A/CN.9/1005, párr. 112; A/CN.9/1087, párr. 19.

“Comprobación de la identidad”

88. El término “comprobación de la identidad” se refiere a la primera etapa de la gestión de la identidad e incluye la inscripción, que es el proceso utilizado por los

[25] Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (“Reglamento eIDAS”).

proveedores de servicios de gestión de la identidad para verificar la identidad que declara un sujeto antes de emitirle una credencial. El sujeto puede ser una persona física o jurídica. El término “comprobación de la identidad” se utiliza en lugar del término “identificación” en respuesta a las preocupaciones expresadas sobre los múltiples significados de “identificación”.

Referencias

A/CN.9/1005, párr. 84.

“Parte que confía”

89. El término “parte que confía” se refiere a una persona física o jurídica que actúa en los hechos en función del resultado de un servicio de gestión de la identidad o un servicio de confianza. Por ejemplo, la parte que confía es una persona que actúa sobre la base de una firma electrónica, y no en función del servicio de confianza utilizado para crear la firma electrónica. La definición se basa en la que figura en el artículo 2 f) de la LMFE.

Referencias

A/CN.9/1087, párrs. 55 y 72.

“Usuario”

90. El término “usuario” se refiere a la persona a quien se prestan los servicios y no incluye a las partes que confían. Supone la existencia de una relación entre el proveedor de servicios y el usuario, que puede ser de carácter contractual o de otra índole (p. ej., dispuesta por la ley). Por ejemplo, el firmante de una firma electrónica queda comprendido en la definición de “usuario”.

Referencias

A/CN.9/1005, párrs. 43 y 96; A/CN.9/1045, párrs. 18 y 22; A/CN.9/1087, párr. 23.

“Servicio de confianza”

91. La definición de “servicio de confianza” combina una descripción abstracta de la función que se persigue con la utilización de servicios de confianza —que se centra en un servicio que proporciona la garantía de calidad de los datos, como la veracidad y la autenticidad— con una lista no taxativa de los servicios de confianza que se prevén expresamente en la Ley Modelo. La adopción de una lista no taxativa permitirá aplicar las normas generales sobre servicios de confianza a otros tipos de servicios de confianza que surjan en el futuro.

92. La referencia a los “métodos para crear y gestionar” deja en claro que el concepto de “servicio de confianza” se refiere a los servicios prestados y no al resultado de la utilización de esos servicios. El servicio de confianza no es, por ejemplo, la firma electrónica en sí misma (es decir, los datos que identifican al firmante y que indican la voluntad que este tiene respecto de la información contenida en el mensaje de datos conexo), sino el servicio que respalda la firma electrónica (es decir, el servicio que proporciona los métodos para que el firmante cree la firma electrónica y dé garantías del cumplimiento de las funciones que se requieren de la firma electrónica).

Referencias

A/CN.9/965, párrs. 101 a 106; A/CN.9/971, párrs. 110 y 111; A/CN.9/1005, párrs. 14 a 18; A/CN.9/1051, párrs. 35 a 40.

“Proveedor de servicios de confianza”

93. El proveedor de servicios de confianza es una persona física o jurídica que presta servicios de confianza. Un prestador de servicios de certificación en el sentido de lo

dispuesto en la LMFE es un ejemplo de proveedor de servicios de confianza con respecto a las firmas electrónicas. A diferencia de lo que ocurre con los proveedores de servicios de gestión de la identidad (art. 6), en la Ley Modelo no se indican las funciones que habrán de desempeñar los proveedores de servicios de confianza. La mención de la existencia de un acuerdo con el usuario es un recordatorio de que el proveedor de servicios de confianza es responsable de todo el conjunto de servicios prestados, independientemente de que las funciones conexas sean cumplidas directamente, o por terceros en calidad de contratistas.

94. La Ley Modelo no exige que se utilicen servicios de confianza prestados por un tercero como condición para obtener el reconocimiento jurídico. Si no se utilizan servicios de confianza prestados por un tercero, la misma entidad puede desempeñar las funciones de proveedor de servicios de confianza y de usuario.

Referencias

A/CN.9/1087, párr. 22.

2. Artículo 2. Ámbito de aplicación

95. El artículo 2 delimita el ámbito de aplicación de la Ley Modelo haciendo referencia a la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza en el contexto de actividades comerciales y servicios relacionados con el comercio. Con el término “servicios relacionados con el comercio” se pretende abarcar las operaciones que están estrechamente relacionadas con el comercio pero que no son de carácter comercial. En esas operaciones pueden participar entidades públicas, como organismos aduaneros que funcionan con una ventanilla única para los trámites de importación y exportación.

96. Dado que el uso de la gestión de la identidad y los servicios de confianza tiene repercusiones que van más allá de las operaciones comerciales, las jurisdicciones promulgantes pueden ampliar el ámbito de aplicación de la Ley Modelo para que abarque todos los tipos de operaciones electrónicas en las que participen empresas, organismos públicos o consumidores.

97. En consonancia con el principio general que inspira los textos de la CNUDMI sobre comercio electrónico, que es favorable a evitar o reducir al mínimo la introducción de modificaciones en el derecho sustantivo vigente, en el párrafo 2 a) se aclara que la Ley Modelo no establece ninguna obligación nueva de identificar.

98. En el párrafo 3 se preservan las obligaciones legales de utilizar un determinado procedimiento de identificación o un servicio de confianza específico. Esas obligaciones, que suelen estar previstas en la reglamentación, incluyen, por ejemplo, la de presentar un documento de identidad específico (p. ej., un pasaporte) o un documento de identidad con determinadas características correspondientes a atributos pertinentes (p. ej., una cédula de identidad con foto y fecha de nacimiento del titular). Las obligaciones de identificar también pueden exigir que la identificación sea realizada por una persona determinada con funciones específicas. Cuando se admite la identificación electrónica, las entidades reguladoras suelen exigir que se utilice un determinado procedimiento de gestión de la identidad o un servicio de confianza específico, como credenciales de identidad emitidas por un organismo público.

99. Dado su carácter facilitador, la Ley Modelo, al igual que los textos legislativos vigentes de la CNUDMI sobre comercio electrónico, no afecta a la aplicación a la gestión de la identidad y los servicios de confianza de otras normas jurídicas que puedan regir esas actividades o algunos aspectos sustantivos de las operaciones realizadas utilizando servicios de identidad o de confianza. En el párrafo 4 se cita en particular ese principio con respecto a las leyes de protección y privacidad de los datos, que se mencionan concretamente debido a su pertinencia. La disposición no se refiere a la privacidad en otros contextos.

Referencias

A/74/17, párr. 172; A/CN.9/936, párr. 52; A/CN.9/965, párr. 125; A/CN.9/971, párr. 23; A/CN.9/1005, párr. 115; A/CN.9/1045, párrs 76 a 78; A/CN.9/1087, párr. 27.

3. Artículo 3. Utilización voluntaria de la gestión de la identidad y los servicios de confianza

100. Según surge del artículo 3, la Ley Modelo no impone el uso de la gestión de la identidad ni de servicios de confianza a ninguna persona que no haya consentido en utilizar la gestión de la identidad o servicios de confianza. Sin embargo, ese consentimiento puede inferirse de la conducta de una parte, por ejemplo, cuando esta opta por utilizar un *software* de comercio electrónico específico o un determinado sistema de comunicaciones electrónicas respaldado por la gestión de la identidad o servicios de confianza.

101. El principio de la utilización voluntaria de la gestión de la identidad y los servicios de confianza está relacionado con el principio de autonomía de las partes, ya que ambos principios se basan en la voluntad. El consentimiento para que se utilice la gestión de la identidad o servicios de confianza puede no coincidir necesariamente con el consentimiento para el tratamiento de información personal conforme a las leyes de protección y privacidad de los datos.

102. El artículo 3, que se basa en el artículo 8, párrafo 2, de la CCE, impide que se imponga cualquier obligación nueva de utilizar la gestión de la identidad o servicios de confianza al usuario, al proveedor de servicios o a la parte que confía. Esta disposición está en consonancia con la norma general de que no se desea modificar el derecho sustantivo.

103. Además, al indicar que la Ley Modelo no exige que se utilice un determinado servicio de gestión de la identidad o servicio de confianza, el artículo 3 aplica el principio de neutralidad tecnológica, en particular con respecto a la neutralidad de los modelos y sistemas.

104. La obligación de utilizar la gestión de la identidad o servicios de confianza, o un determinado servicio de gestión de la identidad o servicio de confianza, puede estar prevista en otras normas jurídicas. Dicha obligación puede imponerse, por ejemplo, respecto de las operaciones que se celebren con entidades públicas o las operaciones que impliquen el cumplimiento de obligaciones previstas en la reglamentación.

Referencias

A/CN.9/965, párrs. 22 y 110; A/CN.9/1005, párr. 116; A/CN.9/1045, párr. 79; A/CN.9/1087, párr. 28.

4. Artículo 4. Interpretación

105. El artículo 4 se basa en las disposiciones de varios tratados y leyes modelo anteriores de la CNUDMI, entre ellos los relativos al comercio electrónico (LMCE, art. 3; LMFE, art. 4; CCE, art. 5; LMDTE, art. 3).

106. El párrafo 1 tiene por objeto promover una interpretación uniforme en todas las jurisdicciones promulgantes y, con ese fin, señala a la atención de los jueces y otros órganos decisorios que las leyes por las que se incorpore la Ley Modelo al derecho interno deben interpretarse teniendo presente su origen internacional y la necesidad de uniformidad en su aplicación. Por lo tanto, se alienta a los decisores a tomar en cuenta las resoluciones dictadas en jurisdicciones extranjeras a la hora de dirimir controversias, a fin de contribuir a consolidar las tendencias transnacionales en materia de interpretación uniforme.

107. El objetivo del párrafo 2 es mantener la uniformidad en la interpretación y la aplicación de las leyes por las que se incorpore la Ley Modelo al derecho interno, exigiendo que las cuestiones que no estén expresamente resueltas en ella se diriman de

conformidad con los principios generales en que se basa la Ley Modelo, y no con arreglo a principios consagrados en el derecho interno.

108. Al igual que otros textos legislativos de la CNUDMI sobre comercio electrónico, la Ley Modelo no indica expresamente los principios generales en que se basa. Los principios de no discriminación contra el uso de medios electrónicos, neutralidad tecnológica, equivalencia funcional y autonomía de las partes suelen estar en la base de los textos legislativos de la CNUDMI sobre comercio electrónico, y se ha entendido que también son aplicables a la Ley Modelo, con las adaptaciones correspondientes (véanse los párrs. 41 a 45 *supra*). Por ejemplo, aunque la autonomía de las partes es un principio fundamental del derecho mercantil, su aplicación está sujeta a las limitaciones establecidas en normas jurídicas imperativas, entre ellas las disposiciones de la Ley Modelo que las partes no pueden excluir. Además, como ya se señaló (párr. 46 *supra*), el principio de equivalencia funcional puede no ser aplicable cuando no existe un requisito fuera de línea.

Referencias

A/CN.9/936, párrs. 67 y 72; A/CN.9/1005, párrs. 117 y 118; A/CN.9/1051, párrs. 53 a 56.

B. Capítulo II. Gestión de la identidad (artículos 5 a 12)

1. Artículo 5. Reconocimiento jurídico de la gestión de la identidad

109. El artículo 5 otorga reconocimiento jurídico a la gestión de la identidad al indicar que el hecho de que la comprobación de la identidad y la identificación electrónica estén en forma electrónica no las priva por sí mismo de efectos jurídicos, validez, fuerza ejecutoria ni admisibilidad como prueba. De ese modo, pone en práctica el principio general de no discriminación contra el uso de medios electrónicos con respecto a la gestión de la identidad. El principio se aplica independientemente de la existencia de un equivalente fuera de línea.

110. El artículo 5 prohíbe discriminar la identificación electrónica cuando esta es el resultado de un proceso de gestión de la identidad. En el título de este artículo se hace referencia al “reconocimiento jurídico”, en lugar de a la “no discriminación”, para mantener la uniformidad con el título de disposiciones análogas que figuran en textos vigentes de la CNUDMI.

111. En el apartado b) se establece que el hecho de que el servicio de gestión de la identidad no sea un servicio designado no impide su reconocimiento jurídico. En otras palabras, el apartado b) otorga el mismo reconocimiento jurídico a los servicios de gestión de la identidad designados, que a los que no han sido designados, garantizando así la neutralidad con respecto al criterio elegido para determinar la fiabilidad. Sin embargo, lo dispuesto en el apartado b) no implica que cualquier servicio de gestión de la identidad utilice métodos fiables y que, por ende, ofrezca un nivel de garantía suficiente para la identificación electrónica: para lograr ese resultado, es necesario evaluar la fiabilidad del método utilizado de acuerdo con los artículos 10 y 11, según el caso.

112. La referencia al artículo 2, párrafo 3, que figura en el encabezamiento del artículo 5 pone de relieve que el artículo 5 no afecta a ninguna obligación legal de identificar a una persona de conformidad con un procedimiento definido o establecido en la ley. El párrafo 3 del artículo 2 se aplica no solamente al artículo 5 sino a todas las demás disposiciones de la Ley Modelo.

Referencias

A/CN.9/965, párrs. 107 y 108; A/CN.9/1005, párrs. 79 a 86; A/CN.9/1045, párrs. 17 y 82 a 84.

2. Artículo 6. Obligaciones de los proveedores de servicios de gestión de la identidad

113. En el artículo 6 figura una lista de las obligaciones de los proveedores de servicios de gestión de la identidad. En esa lista se indican las obligaciones fundamentales del proveedor de servicios de gestión de la identidad, que pueden complementarse con otras obligaciones legales o contractuales. De las palabras “como mínimo” que figuran en el encabezamiento del artículo 6 se infiere que el proveedor de servicios de gestión de la identidad no puede eximirse del cumplimiento de esas obligaciones básicas, sino que es siempre responsable frente a los usuarios y a las partes que confían, también cuando recurre a contratistas para que presten los servicios. El incumplimiento de esas obligaciones puede acarrear responsabilidad conforme a lo dispuesto en el artículo 12 y afectar a la fiabilidad del servicio de gestión de la identidad, aunque se trate de un servicio designado.

114. Las obligaciones previstas en el artículo 6 se describen de manera neutral desde el punto de vista de la tecnología, ya que para que pueda aplicarse el principio de neutralidad tecnológica en el contexto de la gestión de la identidad es necesario que el sistema de gestión de la identidad cumpla unos requisitos mínimos que guardan relación con las propiedades del sistema y no con tecnologías específicas.

115. Además, el artículo 6 tiene por objeto asegurar que el proveedor de servicios de gestión de la identidad siga siendo responsable de todo el conjunto de servicios de gestión de la identidad prestados al usuario, aunque algunas funciones puedan ser desempeñadas por otras entidades, como contratistas o determinados proveedores de servicios de gestión de la identidad que participen en sistemas pluripartitos de gestión de la identidad del sector privado. Por lo tanto, las palabras “como mínimo” que figuran en el apartado a) indican que el proveedor de servicios de gestión de identidad debe contar con normas, políticas y prácticas que reúnan los requisitos exigidos para desempeñar las funciones mencionadas. El artículo 6 no impide que el proveedor de servicios de gestión de la identidad tercerice cualquiera de sus funciones o distribuya el riesgo entre sus contratistas u otros socios comerciales.

116. El principio de que el proveedor de servicios debe quedar obligado por las declaraciones que haga y los compromisos que contraiga ya está consagrado en el artículo 9 a) de la LMFE, que establece la obligación del prestador de servicios de certificación de “actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas”.

117. Los sistemas de gestión de la identidad pueden variar considerablemente en cuanto a sus fines y diseño y en cuanto a los servicios que ofrecen. A su vez, el diseño de un sistema de gestión de la identidad puede depender también del modelo elegido. En consecuencia, es posible que no todas las obligaciones enumeradas en el artículo 6 sean aplicables a todos los proveedores de servicios de gestión de la identidad: más bien, el diseño del sistema de gestión de la identidad y el tipo de servicios de gestión de la identidad prestados determinarán qué obligaciones serán aplicables a un determinado proveedor de servicios de gestión de la identidad. Esa flexibilidad en el diseño del enfoque de los sistemas de gestión de la identidad se refleja en las palabras “que resulten apropiadas para los fines y el diseño”.

118. En la práctica empresarial, las funciones mencionadas en el artículo 6 se rigen comúnmente por normas de funcionamiento de base contractual, sobre todo en el caso de los proveedores de servicios de gestión de la identidad del sector privado. Esas normas, que orientan sobre la forma de realizar las operaciones, se basan en políticas, se aplican mediante prácticas y se recogen en los acuerdos contractuales. La obligación de “tener en vigor normas operacionales, políticas y prácticas” reconoce esa práctica empresarial. Dada la importancia jurídica y práctica de las normas operacionales, políticas y prácticas, en el apartado d) se establece que debería facilitarse el acceso de los usuarios y los terceros a ellas. La referencia a la facilidad de acceso, que figura también en el apartado e), tiene por objeto facilitar el acceso a la información de las partes, como las microempresas o las pequeñas empresas, que pueden estar menos familiarizadas con los aspectos técnicos.

119. En el apartado e) se establecen las obligaciones que deben cumplir los proveedores de servicios de gestión de la identidad para poder limitar su responsabilidad frente a las partes que confían, complementando así el artículo 12. Con este mecanismo se trata de evitar las dificultades que se plantean cuando se exige la identificación de todas las posibles partes que confían antes de que estas actúen en base a esa confianza.

120. De manera similar, el apartado f) complementa el artículo 8 al establecer las obligaciones que debe cumplir el proveedor de servicios de gestión de la identidad cuando un usuario notifica una falla de seguridad.

Referencias

A/CN.9/936, párr. 69; A/CN.9/1045, párrs. 85 a 95; A/CN.9/1087, párrs. 30 a 33, 55 y 61.

3. Artículo 7. Obligaciones de los proveedores de servicios de gestión de la identidad en caso de violación de los datos

121. En el artículo 7 se establecen las obligaciones fundamentales que incumben a los proveedores de servicios de gestión de la identidad cuando se produce una violación de los datos que tiene un impacto considerable en el sistema de gestión de la identidad. Las obligaciones previstas en el artículo 7 se aplican con independencia de los fines y el diseño del sistema de gestión de la identidad y no pueden modificarse por la vía del contrato, ni en las normas operacionales. Las fallas de seguridad pueden afectar tanto a los sistemas como a los servicios de gestión de la identidad y pueden repercutir también en los atributos que se gestionan en el sistema de gestión de la identidad.

122. El concepto de "violación de los datos" se refiere a una falla de seguridad que dé lugar, accidentalmente o de manera ilícita, a la destrucción, pérdida, alteración o divulgación no autorizada de los datos transmitidos, almacenados o procesados de otro modo, o que permita el acceso accidental o ilícito a esos datos. También puede estar definido en las leyes de protección y privacidad de los datos.

123. La noción de "impacto considerable" (o "significativo") se utiliza en la legislación regional [26] y en leyes nacionales. Hay varios factores que pueden contribuir a la evaluación del impacto. Los formularios de notificación de fallas pueden ayudar a evaluar el impacto, aclarando su duración, el tipo de datos y el porcentaje de usuarios afectados y aportando otra información de interés. También se pueden obtener, de las entidades competentes en materia de protección y privacidad de los datos, directrices técnicas para la notificación de incidentes e informes anuales sobre incidentes de seguridad.

124. Habida cuenta de que podría ser conveniente adoptar medidas distintas de la suspensión total, el artículo 7 exige al proveedor de servicios de gestión de la identidad que "tom[e] todas las medidas razonables" para contrarrestar y contener las fallas de seguridad.

125. En el párrafo 1 c) se establece la obligación de notificar las fallas de seguridad, que es uno de los aspectos del principio de transparencia. Es importante contar con un mecanismo adecuado para la notificación de las fallas de seguridad a fin de mejorar el desempeño y aumentar el nivel de confianza en la gestión de la identidad y los servicios de confianza.

126. El artículo 7 se aplica de manera concurrente con las leyes de protección y privacidad de los datos y con cualquier otra norma jurídica aplicable al incidente de que se trate. Por ejemplo, la notificación de incidentes de violación de los datos tiene elementos en común con la notificación de fallas de seguridad, pero también diferencias importantes.

127. Algunos aspectos de las obligaciones establecidas en el artículo 7, como la identificación de las partes a quienes deben notificarse las fallas de seguridad, el momento y el contenido de la notificación, y la divulgación de información sobre la

[26] Reglamento eIDAS, art. 19, párr. 2.

falla y sus detalles técnicos, pueden estar previstos en otras normas jurídicas —a saber, en las leyes de protección y privacidad de los datos—, en acuerdos contractuales y en las normas operacionales, políticas y prácticas del proveedor de servicios de gestión de la identidad. En ese caso, todas las medidas mencionadas en el artículo 7, y no solo la notificación, deberían ejecutarse de conformidad con el derecho aplicable.

Referencias

A/CN.9/971, párrs. 84 a 87; A/CN.9/1005, párrs. 32 a 36 y 94; A/CN.9/1045, párrs. 96 a 101; A/CN.9/1087, párr. 35.

4. Artículo 8. Obligaciones de los usuarios

128. En el artículo 8 se establecen las obligaciones de notificar que incumben a los usuarios cuando las credenciales de identidad se ven comprometidas, o corren el riesgo de verse comprometidas. Esas obligaciones complementan las del proveedor de servicios de gestión de la identidad de proporcionar un medio de notificar las fallas de seguridad (art. 6 f)) y de reaccionar ante cualquier falla de seguridad o pérdida de integridad (art. 7).

129. La obligación del usuario en caso de violación de los datos surge cuando las credenciales de identidad se han visto comprometidas, o cuando existe una gran posibilidad de que se hayan visto comprometidas. Este supuesto es, por ende, diferente del supuesto que hace nacer las obligaciones del proveedor de servicios de gestión de la identidad cuando se produce una violación de los datos, es decir, cuando ocurre una falla de seguridad o una pérdida de integridad que tiene un impacto considerable en el servicio de gestión de la identidad. El incumplimiento por parte del usuario de las obligaciones que le impone el artículo 8 no exime necesariamente de responsabilidad al proveedor de servicios de gestión de la identidad.

130. Del contrato entre el usuario y el proveedor de servicios de gestión de la identidad pueden surgir además otras obligaciones para el usuario. Ese contrato también puede contener información adicional sobre el modo de cumplir la obligación de notificar prevista en el artículo 8.

131. La referencia al empleo de “otros medios razonables” indica que los canales de comunicación que puede utilizar el usuario no se limitan únicamente a los proporcionados por el proveedor de servicios de gestión de la identidad. El concepto de “credenciales de identidad comprometidas” se refiere a los casos de acceso no autorizado a las credenciales de identidad.

132. El apartado b) tiene por objeto contemplar los casos en que el usuario no tiene un conocimiento efectivo de que las credenciales se han visto comprometidas, pero tiene motivos para creer que ello puede haber ocurrido. Dicho apartado se inspira en el artículo 8, párrafo 1 b) ii), de la LMFE, en el que se establecen obligaciones similares para el firmante, y su objetivo es evitar que se imponga una expectativa irrazonablemente alta con respecto a los conocimientos técnicos de los usuarios. La obligación de notificar debería nacer solo cuando las circunstancias de que tenga conocimiento el usuario den lugar a dudas justificadas sobre el funcionamiento correcto de las credenciales de identidad.

Referencias

A/CN.9/936, párr. 68; A/CN.9/971, párrs. 88 a 96; A/CN.9/1005, párrs. 37 a 43, 95 y 96; A/CN.9/1045, párrs. 102 a 105; A/CN.9/1087, párrs. 36 y 37.

5. Artículo 9. Identificación de personas mediante la gestión de la identidad

133. En los textos de la CNUDMI sobre comercio electrónico, las normas de equivalencia funcional establecen las condiciones que debe reunir un documento, método o proceso electrónico para cumplir las mismas funciones que el equivalente en papel exigido por la ley. En el artículo 9 se establece una norma de equivalencia funcional para aquellos casos en que la ley exige la identificación, o en que las partes

convienen en identificarse mutuamente. Dado que el objetivo de esta disposición es establecer las condiciones para que exista equivalencia entre la identificación fuera de línea y la identificación en línea, el artículo 9 es aplicable solamente en el caso de que exista un equivalente de identificación fuera de línea. No obstante, el artículo 9 es una disposición fundamental para establecer un régimen jurídico aplicable a la gestión de la identidad.

134. El método utilizado para cumplir con la norma del artículo 9 debe ajustarse a lo dispuesto en el artículo 10, párrafo 1, es decir, ser tan fiable como resulte apropiado para los fines para los que se utiliza el servicio de gestión de la identidad, o haber demostrado en la práctica que ha cumplido la función que se persigue con el uso del método.

135. En consonancia con los principios establecidos en los textos de la CNUDMI, esta norma de equivalencia funcional complementa la norma de reconocimiento jurídico enunciada en el artículo 5. Sin embargo, mientras que el artículo 5 se aplica a todas las formas de identificación electrónica, independientemente de la existencia de un equivalente de identificación fuera de línea, el objeto del artículo 9 es la identificación electrónica como equivalente funcional de la identificación fuera de línea y, por consiguiente, el artículo 9 solo puede aplicarse con referencia a un equivalente en papel.

136. El artículo 9 se refiere al uso de servicios de gestión de la identidad para indicar que los requisitos de equivalencia se cumplen cuando se utilizan credenciales de identidad, a diferencia de cuando se utilizan sistemas de gestión de la identidad o la identidad en sí misma.

137. Lo dispuesto en el artículo 9 es sin perjuicio de las obligaciones de identificar con arreglo a un método o procedimiento determinado, como se establece en el artículo 2, párrafo 3. Esas obligaciones pueden estar relacionadas con el cumplimiento de requisitos de regulación, como los establecidos en la reglamentación bancaria y de lucha contra el blanqueo de dinero (véase el párr. 98 *supra*).

138. La identificación electrónica puede utilizarse para cumplir la obligación de verificar determinados atributos de la identidad de una persona, como la edad o el domicilio, tal como se exige para la identificación física. En tal sentido, dado que el concepto de “identidad” se define en función del “contexto”, que a su vez determina los atributos necesarios para la identificación, la identificación satisfactoria de una persona sobre la base del artículo 9 incluye la verificación de los atributos exigidos. La necesidad de verificar los atributos pertinentes se refleja también en las palabras “con ese fin”. La verificación de determinados atributos no está prevista en las disposiciones sobre fiabilidad contenidas en el artículo 10, ya que dichas disposiciones se refieren a los procesos de gestión de las credenciales de identidad y no a los atributos contenidos en ellas.

139. Los artículos 9 y 16 a 21 de la Ley Modelo se refieren a los casos en que la ley requiere una acción o prevé las consecuencias de su omisión. Se ha empleado esta formulación, que se utiliza en el artículo 9 de la CCE, para permitir la aplicación de normas de equivalencia funcional en los casos en que la ley no exige determinadas acciones, pero las permite y les atribuye consecuencias jurídicas.

Referencias

A/CN.9/965, párrs. 62 a 85; A/CN.9/971, párrs. 24 a 49; A/CN.9/1005, párrs. 97 a 100; A/CN.9/1045, párrs. 106 a 117; A/CN.9/1051, párrs. 42 a 44; A/CN.9/1087, párr. 38.

6. Artículo 10. Requisitos de fiabilidad de los servicios de gestión de la identidad

140. El artículo 10 ofrece orientación sobre la forma de determinar la fiabilidad del método utilizado para la identificación, mencionado en el artículo 9, después de utilizado dicho método (criterio *ex post*). Se refiere al método utilizado en un servicio de gestión de la identidad, más que al método utilizado en un sistema de gestión de la identidad, porque un mismo sistema de gestión de la identidad podría respaldar varios

servicios de gestión de la identidad que utilizaran métodos con diferentes niveles de fiabilidad.

141. En el párrafo 1 a) se aplica el criterio *ex post* al hacerse referencia al empleo de un método que sea "tan fiable como resulte apropiado para los fines para los que se utiliza el servicio de gestión de la identidad". Esta disposición refleja el entendimiento de que la fiabilidad es un concepto relativo. Sin embargo, a diferencia de algunos servicios de confianza que pueden cumplir varias funciones, la identificación electrónica persigue una sola función, que es la identificación fiable por medios electrónicos. Esa función puede tener diversos fines, cada uno de ellos vinculado a un nivel de fiabilidad diferente.

142. En el párrafo 1 b) figura una disposición que tiene por objeto evitar que se rechace un servicio de gestión de la identidad cuando en la práctica ha cumplido su función. El rechazo se produce cuando un sujeto declara no haber realizado una acción. Para que el mecanismo previsto en el párrafo 1 b) funcione, el método, sea fiable o no, debe haber cumplido en la práctica la función de identificación, es decir, vincular a la persona que solicita la identificación con las credenciales de identidad. Esta disposición se basa en el artículo 9, párrafo 3 b) ii), de la CCE.

143. La Ley Modelo exige en general que se utilicen métodos fiables, y el párrafo 1 b) no pretende fomentar el empleo de métodos no fiables, ni validar el uso de esos métodos. Por el contrario, reconoce que, desde una perspectiva técnica, la función (en el caso del artículo 9, la identificación) y la fiabilidad son dos atributos independientes, y aclara que, de acuerdo con la Ley Modelo, la identificación puede lograrse en la práctica o mediante el uso de un método fiable. En otras palabras, cuando se logra la identificación en la práctica, se elimina la necesidad de comprobar la fiabilidad del método utilizado.

144. En el párrafo 2 figura una lista de circunstancias, descritas en términos neutrales desde el punto de vista de la tecnología, que pueden ser pertinentes para la determinación de la fiabilidad por el órgano decisor. Dado que la lista es a vía de ejemplo y no taxativa, puede haber otras circunstancias que también sean pertinentes. Además, no todas las circunstancias mencionadas pueden ser pertinentes en todos los casos en que haya que determinar la fiabilidad. En particular, la relevancia del acuerdo existente entre las partes puede variar considerablemente en función del grado de reconocimiento que cada jurisdicción otorgue a la autonomía de las partes en el ámbito de la identificación. Además, los acuerdos contractuales pueden no afectar a terceros, por lo que esa circunstancia no sería relevante cuando intervinieran terceros.

145. En el párrafo 3 se establece que el lugar donde se preste el servicio de gestión de la identidad y la ubicación del establecimiento del proveedor de servicios de gestión de la identidad son en sí mismas irrelevantes a los efectos de determinar la fiabilidad. Esta disposición tiene por objeto facilitar el reconocimiento transfronterizo de los servicios de gestión de la identidad y se inspira en el artículo 12, párrafo 1, de la LMFE, que establece una norma general de no discriminación para determinar los efectos jurídicos de un certificado o una firma electrónica[27].

146. Según el párrafo 4, la designación de un servicio de gestión de la identidad fiable de conformidad con el artículo 11 otorga una presunción de fiabilidad a los métodos utilizados por el servicio de gestión de la identidad designado. Esa es la única distinción entre los servicios de gestión de la identidad designados y los no designados. Además, de acuerdo con el párrafo 5 b), la presunción de fiabilidad otorgada a la designación puede rebatirse.

147. En el párrafo 5 se aclara la relación entre los artículos 10 y 11 al establecerse que la existencia de un mecanismo de designación no excluye la posibilidad de que se haga una determinación *ex post* de la fiabilidad del método. Esta disposición se inspira en el artículo 6, párrafo 4, de la LMFE.

[27] En el documento A/CN.9/483, párrs. 28 a 36, se analiza la interacción entre los párrafos 1 y 2 del artículo 12 de la LMFE.

a) Marco de niveles de garantía

148. En los artículos 10 y 11 se hace referencia al concepto de “marcos de niveles de garantía” o a marcos similares denominados de otro modo. El marco de niveles de garantía ofrece orientación a las partes que confían sobre el grado de confianza que pueden depositar en los procesos de comprobación de la identidad y de identificación electrónica y sobre si esos procesos son adecuados para determinados fines. La Ley Modelo no define los niveles de garantía ni exige que se definan o utilicen.

149. Los marcos de niveles de garantía prevén distintos niveles de garantía que se asocian a diferentes requisitos. En otras palabras, los marcos de niveles de garantía describen los requisitos que deben cumplir los sistemas y servicios de gestión de la identidad para proporcionar un determinado nivel de garantía en cuanto a su fiabilidad. Los niveles de garantía deberían describirse en términos genéricos para mantener la neutralidad tecnológica.

150. Los marcos de niveles de garantía pueden utilizarse como medio de responder a la necesidad del mercado de recibir orientación sobre el grado de fiabilidad de los servicios de gestión de la identidad ofrecidos. Si un proveedor de servicios de gestión de la identidad no menciona los niveles de garantía en sus normas operacionales, políticas y prácticas, podría considerarse que los servicios que ofrece son del nivel de garantía más bajo. Sin embargo, es posible que aún no se haya acordado una definición de marco de niveles de garantía aceptada universalmente y que haya que utilizar diferentes definiciones nacionales o regionales.

151. A su vez, la necesidad de que exista un determinado nivel de garantía de la fiabilidad de las identidades utilizadas puede expresarse con referencia a los niveles descritos en un marco de niveles de garantía. Posteriormente, se pueden clasificar determinados sistemas y servicios de gestión de la identidad en función de los requisitos exigidos con respecto al nivel de garantía. Cuando un servicio de gestión de la identidad se ajusta a los requisitos asociados a ese nivel de garantía surge la posibilidad de utilizar ese servicio de gestión de la identidad para ese tipo de operación en particular.

b) Certificación y supervisión

152. En el artículo 10 se menciona, entre las posibles circunstancias pertinentes, la existencia de una “supervisión o certificación que se hubiera realizado con respecto al servicio de gestión de la identidad”. La certificación y la supervisión pueden ayudar en gran medida a generar confianza en los proveedores de servicios de gestión de la identidad y en los servicios que estos prestan, incluso a los efectos de determinar la fiabilidad del método utilizado, ya que se asocian a un cierto grado de objetividad en la evaluación de la fiabilidad del método utilizado. Esto ya se reconoció en el artículo 12 a) vi) de la LMDTE y en el artículo 10 f) de la LMFE.

153. Las opciones de certificación son, entre otras, la autocertificación, la certificación por un tercero independiente, la certificación por un tercero independiente acreditado y la certificación por una entidad pública. En la elección de la forma más apropiada de certificación influyen el tipo de servicio de que se trate, el costo y el nivel de garantía deseado. En el contexto de las operaciones entre empresas, los socios comerciales deberían poder elegir la opción más acorde con sus necesidades, teniendo en cuenta que cada opción producirá efectos diferentes.

154. La existencia de un mecanismo de supervisión de los sistemas y servicios de gestión de la identidad puede considerarse útil o incluso necesaria para generar confianza en la gestión de la identidad. Sin embargo, la creación de un órgano de supervisión tiene consecuencias administrativas y financieras que pueden ser costosas.

155. Existen diferentes criterios en lo que respecta a la participación de entidades públicas en la certificación y la supervisión, y esa es una decisión de política que tendrá que adoptar la jurisdicción promulgante. Cuando las entidades públicas son certificadoras o supervisoras y, al mismo tiempo, proveedoras de servicios de gestión de la identidad, las funciones de certificación y supervisión pueden separarse de la prestación de servicios de gestión de la identidad.

156. La Ley Modelo no ordena ni facilita el establecimiento de un régimen de supervisión. El criterio adoptado en la Ley Modelo se basa en la neutralidad del modelo y las referencias a la certificación y la supervisión no excluyen los regímenes de autocertificación.

157. En algunos casos, como cuando se utilizan determinados tipos de tecnología de registros distribuidos, una solución que entrañe la intervención de un órgano central de certificación, acreditación o supervisión puede no ser apropiada debido a las dificultades para determinar cuál es la entidad que puede solicitar la certificación, la entidad que debe ser evaluada y la entidad encargada de adoptar medidas correctivas y de ejecución, entre otras.

Referencias

A/CN.9/965, párrs. 40 a 55 y 112 a 115; A/CN.9/971, párrs. 50 a 61; A/CN.9/1005, párr. 101; A/CN.9/1045, párrs. 118 a 124; A/CN.9/1051, párrs. 47 a 49; A/CN.9/1087, párrs. 42 a 46, 105 y 106; A/CN.9/WG.IV/WP.153, párrs. 74 y 75.

7. Artículo 11. Designación de servicios de gestión de la identidad fiables

158. El artículo 11 complementa el artículo 10 al ofrecer la posibilidad de designar servicios de gestión de la identidad. Más concretamente, establece las condiciones que debe reunir un servicio de gestión de la identidad para ser incluido en una lista de servicios de gestión de la identidad designados. Al igual que el artículo 10, el artículo 11 se refiere al método utilizado en un servicio de gestión de la identidad, más que al método utilizado en un sistema de gestión de la identidad, porque un mismo sistema de gestión de la identidad podría respaldar varios servicios de gestión de la identidad con diferentes niveles de fiabilidad que, por lo tanto, podrían haber sido designados o no.

159. La designación de servicios de gestión de la identidad que utilizan métodos fiables se basa en todas las circunstancias pertinentes, entre ellas las mencionadas en el artículo 10 como circunstancias que deben tenerse en cuenta para determinar la fiabilidad del método. La referencia a las circunstancias mencionadas en el artículo 10 garantiza cierto grado de coherencia entre los métodos designados como fiables *ex ante* y los métodos determinados como fiables *ex post*. Además, la designación debe "ajustarse a las normas y procedimientos internacionales reconocidos que sean pertinentes para llevar a cabo el proceso de designación", a fin de promover el reconocimiento jurídico transfronterizo y la interoperabilidad.

160. La difusión de información sobre los servicios de gestión de la identidad designados es fundamental para que los posibles usuarios conozcan su existencia. La entidad designadora tiene la obligación de publicar, por ejemplo en su sitio web, una lista de los servicios de gestión de la identidad designados, con detalles de los proveedores de esos servicios. La importancia de las listas para garantizar la transparencia en la designación de los servicios de gestión de la identidad, en particular en el contexto transfronterizo, está reconocida también en normas técnicas ampliamente utilizadas. Se pueden emplear otros métodos para informar al público acerca de los servicios de gestión de la identidad designados, pero esos métodos deberían complementar y no sustituir la publicación de una lista.

161. El párrafo 2 a) se refiere a las normas y procedimientos pertinentes para determinar la fiabilidad y su objetivo es garantizar cierta uniformidad en el resultado de las evaluaciones *ex ante* y *ex post* de la fiabilidad. Por otra parte, en el párrafo 3 se mencionan expresamente las normas y procedimientos pertinentes para la designación, como las evaluaciones de la conformidad y las auditorías, que son propias del criterio *ex ante*.

162. Al igual que en el párrafo 3 del artículo 10, en el párrafo 4 se establece que el lugar donde se preste el servicio de gestión de la identidad y la ubicación del establecimiento del proveedor de servicios de gestión de la identidad son de por sí irrelevantes a los efectos de designar un servicio fiable. El párrafo 4 se basa en el artículo 12, párrafo 1, de la LMFE, que establece una norma general de no discriminación para determinar los

efectos jurídicos de un certificado o una firma electrónica. En la práctica, esta disposición permite que un proveedor de servicios de gestión de la identidad extranjero solicite a la autoridad competente de la jurisdicción promulgante la designación del servicio de gestión de la identidad.

Referencias

A/CN.9/965, párrs. 40 a 55; A/CN.9/971, párrs. 68 a 76; A/CN.9/1005, párrs. 102 y 105; A/CN.9/1045, párrs. 125 a 129; A/CN.9/1087, párrs. 47 a 49.

8. Artículo 12. Responsabilidad de los proveedores de servicios de gestión de la identidad

163. Como ya se señaló (párr. 68 *supra*), el artículo 12 establece un régimen de responsabilidad uniforme basado en el principio de que un proveedor de servicios de gestión de la identidad debe responder de las consecuencias de la falta de prestación de los servicios a los usuarios y a las partes que confían. Su objetivo es reconocer que el proveedor de servicios puede incurrir en responsabilidad por el incumplimiento de las obligaciones que le impone la Ley Modelo, independientemente de que esas obligaciones tengan o no un fundamento contractual. La disposición se aplica con independencia del carácter público o privado del proveedor de servicios de gestión de la identidad.

164. El artículo 12 se basa en tres elementos: a) no afecta a la aplicación de las normas jurídicas imperativas, entre ellas las disposiciones de la Ley Modelo que imponen obligaciones inderogables al proveedor de servicios de gestión de la identidad; b) establece la responsabilidad del proveedor de servicios de gestión de la identidad por el incumplimiento de sus obligaciones inderogables, independientemente de que dichas obligaciones tengan también un fundamento contractual, y c) reconoce la posibilidad de limitar la responsabilidad siempre y cuando se cumplan determinadas condiciones.

165. La responsabilidad prevista en el artículo 12 es de carácter legal y, como tal, se aplica junto con la responsabilidad contractual y extracontractual. Por consiguiente, el artículo 12 no afecta a la aplicación de las disposiciones sobre responsabilidad contractual y extracontractual que sean pertinentes para los proveedores de servicios de gestión de la identidad y que estén previstas en el derecho interno, como se indica en el párrafo 2 a).

166. Los proveedores de servicios de gestión de la identidad pueden incurrir en responsabilidad como consecuencia de la utilización de servicios de gestión de la identidad tanto designados como no designados. Sin embargo, esa responsabilidad no es absoluta. Por ejemplo, un proveedor de servicios de gestión de la identidad puede no ser responsable frente a un usuario si la pérdida fue causada por la utilización de credenciales que el usuario, en el momento de utilizarlas, sabía o debería haber sabido que se habían visto comprometidas.

167. Las cuestiones relativas a la responsabilidad que no estén contempladas en el artículo 12 se dejan en manos del derecho que resulte aplicable más allá del proyecto de disposiciones. Esas cuestiones son, entre otras, el grado de diligencia, el grado de culpa, la carga de la prueba y la determinación del monto de los daños y perjuicios y de la indemnización.

168. En el artículo 12 se reconoce la posibilidad de limitar la responsabilidad si se cumplen determinadas condiciones. Puede ser necesario limitar la responsabilidad para moderar el costo de los seguros, entre otras cosas, y esas limitaciones suelen estar previstas en las normas operacionales, políticas y prácticas del proveedor de servicios. En el artículo 12 se reconoce también que, en la práctica, los proveedores de servicios de gestión de la identidad limitan su responsabilidad de manera diferente según quién sea la contraparte (es decir, el usuario o la parte que confía) y en función del tipo de servicio (p. ej., operación de alto valor o de poco valor). El artículo 12 no impide que el proveedor de servicios de gestión de la identidad invoque otras leyes para aplicar un

límite a su responsabilidad, siempre y cuando cumpla las obligaciones que le impone la Ley Modelo, incluidas las que sean pertinentes para limitar la responsabilidad.

169. Con respecto al usuario, el párrafo 3 permite limitar la responsabilidad del proveedor de servicios de gestión de la identidad si se cumplen dos condiciones. En primer lugar, la utilización del servicio de gestión de la identidad debe exceder la limitación en cuanto a los fines o el valor de la operación y al monto de la responsabilidad aplicable a la operación para la que se utiliza el servicio de gestión de la identidad. En segundo lugar, las limitaciones tienen que estar previstas en el acuerdo existente entre el proveedor de servicios de gestión de la identidad y el usuario. En consonancia con la definición de "usuario", la referencia al "acuerdo" pretende captar todo tipo de relación, ya sea de carácter contractual o de otra naturaleza, entre el proveedor de servicios de gestión de la identidad y el usuario.

170. Del mismo modo, el párrafo 4 permite limitar la responsabilidad del proveedor de servicios de gestión de la identidad frente a la parte que confía si se cumplen dos condiciones. En primer lugar, la utilización del servicio de gestión de la identidad debe exceder la limitación en cuanto a los fines o el valor de la operación y al monto de la responsabilidad aplicable a la operación para la que se utiliza el servicio de gestión de la identidad. En segundo lugar, el proveedor de servicios de gestión de la identidad tiene que haber cumplido las obligaciones que le impone el artículo 6 e) en cuanto a facilitar el acceso de las partes que confían a las limitaciones relacionadas con determinada operación.

171. El artículo 12 prevé únicamente la responsabilidad de los proveedores de servicios de gestión de la identidad frente a los usuarios y las partes que confían. Si hubiera otra parte perjudicada por el uso de los servicios de gestión de la identidad, esa parte podría reclamar una reparación al amparo de las normas de responsabilidad vigentes, ya fuese contra el proveedor de servicios o contra el usuario. En este último caso, el usuario podría a su vez reclamar contra el proveedor de servicios de gestión de la identidad.

172. El artículo 12 se aplica a los proveedores de servicios de gestión de la identidad con independencia de que sean de carácter público o privado. Es posible que las jurisdicciones promulgantes tengan que adaptar esta disposición a cualquier norma especial sobre la responsabilidad de las entidades públicas. El artículo 12 no es aplicable a las entidades públicas que desempeñan funciones de supervisión y administran registros civiles y estadísticas vitales que pueden proporcionar credenciales de identidad básicas.

Referencias

A/CN.9/936, párrs. 83 a 86; A/CN.9/965, párrs. 116 a 118; A/CN.9/971, párrs. 98 a 107; A/CN.9/1005, párr. 76; A/CN.9/1045, párrs. 130 y 131; A/CN.9/1051, párrs. 13 a 29; A/CN.9/1087, párrs. 52 a 73.

C. Capítulo III. Servicios de confianza (artículos 13 a 24)

1. Artículo 13. Reconocimiento jurídico de los servicios de confianza

173. El artículo 13 establece una norma general de no discriminación contra el resultado de la utilización de un servicio de confianza, es decir, la afirmación de determinadas propiedades de un mensaje de datos. Al hacer referencia al resultado de la utilización de un servicio de confianza, este artículo recoge el criterio adoptado en el artículo 5, que otorga reconocimiento jurídico a la identificación electrónica como resultado del uso de la gestión de la identidad.

174. El artículo 13 es aplicable a los servicios de confianza, estén o no previstos expresamente en la Ley Modelo, y se aplica independientemente de la existencia de una norma de equivalencia funcional.

Referencias

A/CN.9/971, párrs. 112 a 115; A/CN.9/1005, párrs. 19 a 26; A/CN.9/1045, párrs. 16 y 17.

2. Artículo 14. Obligaciones de los proveedores de servicios de confianza

175. En el artículo 14 se establecen las obligaciones básicas de los proveedores de servicios de confianza, con independencia de que el servicio de confianza prestado esté o no previsto expresamente en la Ley Modelo. Los acuerdos contractuales pueden especificar y complementar esas obligaciones básicas, pero no pueden apartarse de ellas. Este criterio es similar al adoptado en los artículos 6 y 7 en relación con las obligaciones de los proveedores de servicios de gestión de la identidad. Al igual que lo que sucede con el artículo 7, párrafo 1, todas las obligaciones establecidas en el artículo 14, párrafo 2, deben cumplirse de conformidad con la ley aplicable, si la hubiera.

176. Al hacerse referencia a las normas operacionales, políticas y prácticas "que resulten apropiadas para los fines y el diseño del servicio de confianza" se reconoce que las obligaciones de los proveedores de servicios de confianza pueden variar a la luz de las diferencias que existan en el diseño y la función de cada servicio de confianza.

177. La obligación de dar a conocer las políticas y prácticas también a los terceros refleja la práctica actual, según la cual se reconoce que esa información es importante para las partes que confían cuando tienen que decidir si aceptar o no el resultado de la utilización de un servicio de confianza, en consonancia con el principio de la utilización voluntaria de los servicios de confianza (art. 3, párr.1).

178. En el párrafo 1 e) se establece un mecanismo para poner en conocimiento de las partes que confían las limitaciones que existen en cuanto a los fines o el valor para los que puede utilizarse el servicio de confianza, y las limitaciones aplicables al alcance o la magnitud de la responsabilidad, que es similar al mecanismo establecido en el artículo 6 e) y complementa el artículo 24.

179. En el párrafo 2 se establecen las obligaciones de los proveedores de servicios de confianza en caso de violación de los datos. Se contempla la hipótesis de que se produzca una falla de seguridad o una pérdida de integridad que tenga un impacto considerable en el servicio de confianza.

Referencias

A/CN.9/971, párrs. 152 y 153; A/CN.9/1005, párrs. 28 a 36 y 73; A/CN.9/1045, párrs. 18 a 21 y 57; A/CN.9/1087, párrs. 74 a 76.

3. Artículo 15. Obligaciones de los usuarios

180. En el artículo 15 se establecen las obligaciones de los usuarios en el caso de que el servicio de confianza se haya visto comprometido. La noción subyacente de que un servicio de confianza "se vea comprometido" se refiere a los casos de acceso no autorizado al servicio de confianza y parte del supuesto de que ha ocurrido un incidente que afecta a la fiabilidad del servicio de confianza.

181. En el artículo 15 se reconoce que es poco probable que el usuario tenga conocimiento inmediato de los problemas que afectan al servicio de confianza en su totalidad, pero que puede saber que hay información visible que se ha visto comprometida y que tal vez sea consciente de la posibilidad de que la información no visible directamente para el usuario, como una clave privada, corre riesgos. Por ese motivo, los apartados a) y b) tienen dos objetos diferentes.

182. Por lo general, en el contrato celebrado entre el proveedor de servicios de confianza y el usuario se detalla la forma de cumplir las obligaciones enunciadas en el artículo 15. En esos acuerdos contractuales se suele hacer referencia a las normas operacionales, políticas y prácticas del proveedor de servicios de confianza.

183. En la Ley Modelo no se establecen otras obligaciones de los usuarios con respecto a la utilización de los servicios de confianza. Un ejemplo de esa clase de obligaciones puede encontrarse en el artículo 8, párrafo 1 a) y c), de la LMFE.

184. La Ley Modelo no contiene normas que rijan la responsabilidad de los usuarios. Por lo tanto, la responsabilidad de los usuarios se determinará de acuerdo con las cláusulas del contrato —en el que pueden haberse estipulado otras obligaciones de los usuarios— y con arreglo a las normas generales en materia de responsabilidad.

185. A diferencia del artículo 11 de la LMFE, el artículo 15 no impone obligaciones a las partes que confían, las que pueden incurrir en responsabilidad en virtud de lo dispuesto en otras leyes.

Referencias

A/CN.9/1005, párrs. 37 a 43; A/CN.9/1045, párrs. 22 a 26; A/CN.9/1087, párrs. 77 y 78.

4. Artículo 16. Firmas electrónicas

186. El artículo 16 trata de las firmas electrónicas. Todos los textos legislativos de la CNUDMI sobre comercio electrónico contienen disposiciones sobre el uso de las firmas electrónicas, que pueden ser estampadas tanto por personas físicas como jurídicas[28]. En el artículo 16, cuya redacción se inspira en la del artículo 9 de la LMDTE, que a su vez tiene en cuenta la formulación del artículo 9, párrafo 3, de la CCE, se establecen los requisitos de equivalencia funcional entre las firmas manuscritas y las electrónicas. Por lo tanto, el término “identificar”, tal como figura en el artículo 16, debe interpretarse en consonancia con el significado establecido en disposiciones similares de la CNUDMI y en las leyes por las que se han incorporado al derecho interno.

187. El requisito de la firma en papel se cumple si se utiliza un método para identificar al firmante del mensaje de datos y para indicar la voluntad del firmante con respecto al mensaje de datos firmado. La referencia al uso del método “respecto de la información contenida en el mensaje de datos” se aplica tanto a la identificación de la persona como a la indicación de su voluntad.

188. Las firmas electrónicas pueden utilizarse con diversos fines, por ejemplo, para identificar al iniciador de un mensaje y vincularlo a su contenido. Existen varias tecnologías y métodos que pueden cumplir los requisitos de una firma electrónica. En un entorno comercial, las partes pueden determinar cuáles son la tecnología y el método de firma electrónica más adecuados en función de los costos, el nivel de seguridad deseado, la distribución de los riesgos y otras consideraciones. En textos anteriores de la CNUDMI se han analizado en profundidad los fines y los métodos de las firmas electrónicas[29].

Referencias

A/CN.9/971, párrs. 116 a 119; A/CN.9/1005, párrs. 44 a 51; A/CN.9/1045, párr. 34; A/CN.9/1051, párr. 50; A/CN.9/1087, párrs. 82 a 84.

5. Artículo 17. Sellos electrónicos

189. Los sellos electrónicos ofrecen una garantía del origen y la integridad de un mensaje de datos procedente de una persona jurídica. En la práctica, combinan la función de una firma electrónica genérica con respecto al origen, con la de algunos tipos de firma, normalmente basados en el uso de claves criptográficas, con respecto a la integridad. La existencia de esas firmas electrónicas se refleja en el artículo 6, párrafo 3 d), de la LMFE. Por consiguiente, la descripción del requisito de integridad que figura en el artículo 17 se basa en el artículo 6, párrafo 3 d), de la LMFE.

[28] Véase también, en general, el documento *Fomento de la confianza en el comercio electrónico*.

[29] LMFE, *Guía para su incorporación al derecho interno*, párrs. 29 a 62; *Fomento de la confianza en el comercio electrónico*, párrs. 24 a 66.

190. El artículo 17 se inspira en la legislación regional, según la cual “Además de autenticar el documento expedido por la persona jurídica, los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores” (Reglamento eIDAS, considerando 65).

191. La garantía del origen del mensaje de datos puede obtenerse determinando su procedencia, lo que, a su vez, exige identificar a la persona jurídica que inició el mensaje de datos. El método utilizado para identificar a la persona jurídica que estampa el sello es el mismo que se utiliza para identificar a un firmante, y por lo general las disposiciones de la CNUDMI sobre las firmas electrónicas se han incorporado al derecho interno como normas aplicables tanto a las personas físicas como a las jurídicas.

192. Además, las disposiciones de los textos de la CNUDMI exigen la integridad para lograr la equivalencia funcional con el concepto de “original” propio de los documentos en papel. En particular, el artículo 6, párrafo 3 d), de la LMFE se refiere al concepto de “integridad” cuando uno de los objetivos del requisito legal de la firma es dar garantías de la integridad de la información a la que se refiere.

193. En vista de lo anterior, es posible que las jurisdicciones que ya han incorporado a su derecho interno disposiciones de la CNUDMI sobre las firmas electrónicas que dan garantías de integridad no distingan entre las funciones que se persiguen con la utilización de una firma electrónica y las que se persiguen con el uso de un sello electrónico. Esto puede reflejar también la práctica empresarial de utilizar métodos híbridos que combinen firmas electrónicas con sellos electrónicos.

Integridad

194. La integridad es un elemento esencial de los sellos electrónicos y del archivado electrónico y puede ser un elemento opcional de otros servicios de confianza. En textos anteriores de la CNUDMI, la integridad es un requisito para lograr la equivalencia funcional con el concepto de “original” propio de los documentos en papel (LMCE, art. 8). Los artículos 17 y 19 se inspiran en el artículo 8, párrafo 3, de la LMCE en cuanto a los requisitos exigidos para garantizar la integridad.

Referencias

A/CN.9/971, párrs. 124 a 128; A/CN.9/1005, párrs. 52 a 54 y 58; A/CN.9/1045, párrs. 35, 36 y 56 a 58; A/CN.9/1087, párrs. 85 y 86.

6. Artículo 18. Sellos de tiempo electrónicos

195. Los sellos de tiempo electrónicos ofrecen prueba de la fecha y hora en que el sello se vinculó a los datos. Normalmente, la ley atribuye consecuencias al hecho de que la fecha y hora de un determinado acontecimiento no puedan probarse con un nivel de confianza suficiente. Por ejemplo, puede ser necesario probar la fecha de celebración de un contrato para invocar su oponibilidad a terceros.

196. Los sellos de tiempo se estampan normalmente en relación con determinadas acciones, como la generación de un documento electrónico en su forma definitiva, la firma, el envío y la recepción de una comunicación electrónica, etc. El requisito de especificar una zona horaria puede cumplirse haciendo referencia al tiempo universal coordinado (UTC), aunque no necesariamente.

197. En el artículo 18 se mencionan los “datos”, además de los “documento[s] en papel o electrónico[s]” y la “información”. Con ello se trata de contemplar los casos en que los sellos de tiempo están vinculados a datos que no figuran en un documento en papel o electrónico y que no se presentan de manera organizada como información.

Referencias

A/CN.9/971, párrs. 129 a 134; A/CN.9/1005, párr. 55.

7. Artículo 19. Archivado electrónico

198. El artículo 19 trata de los servicios de archivado electrónico, que dan seguridad jurídica con respecto a la validez de los documentos electrónicos conservados. El método utilizado para el archivado electrónico debe garantizar la integridad de los documentos electrónicos archivados, así como de la fecha y hora en que se archivaron. Además, la información archivada debe ser accesible de acuerdo con el requisito de equivalencia funcional con la noción de "escritura" propia de los documentos en papel (LMCE, art. 6, párr. 1).

199. El artículo 19 se inspira, entre otros, en el artículo 10 de la LMCE, que trata de la conservación de los mensajes de datos. Sin embargo, el artículo 10 de la LMCE se refiere a la "conservación" de los mensajes de datos porque trata del cumplimiento de la obligación legal de conservar documentos en papel, mientras que el artículo 19 se refiere al "archivado" porque trata del servicio de confianza prestado para satisfacer ese requisito (es decir, el archivado electrónico).

200. Los mensajes de datos archivados no necesitan haber sido enviados o recibidos y pueden ser conservados por el iniciador.

201. Para transmitir y conservar mensajes de datos puede ser necesario, por razones técnicas, hacer adiciones o modificaciones al mensaje de datos que no alteren su integridad. Esas adiciones y modificaciones están permitidas siempre que el contenido del mensaje de datos se mantenga completo e inalterado. En el apartado c) se contempla la posibilidad de migrar archivos y hacer cambios de formato, operaciones estas que forman parte de las prácticas corrientes de conservación de datos. La redacción de esta norma se basa en la del artículo 8, párrafo 3 a), de la LMCE.

202. En el artículo 19 no se plantea la cuestión de si los documentos electrónicos archivados deben poder ser migrados para que sea posible acceder a ellos a pesar de la obsolescencia tecnológica. Se llega a ese resultado mediante la aplicación al concepto de "integridad" del principio de neutralidad tecnológica y de los requisitos de equivalencia funcional, de manera que, cuando sea necesario presentar información, esta pueda mostrarse a la persona a quien se deba presentar (LMCE, art. 8, párr. 1 b)).

Referencias

A/CN.9/971, párrs. 135 a 138; A/CN.9/1005, párrs. 56 a 61; A/CN.9/1045, párrs. 37 a 41.

8. Artículo 20. Servicios de entrega electrónica certificada

203. En el artículo 20 se establece la forma de garantizar que una comunicación electrónica fue enviada por el remitente y recibida por el destinatario; el momento en que se produjeron el envío y la recepción; la integridad de los datos transmitidos, y la identidad del remitente y del destinatario.

204. Los servicios de entrega electrónica certificada son el equivalente de los servicios de correo certificado, ya que ambos tipos de servicios se utilizan para demostrar la transmisión de comunicaciones. Para garantizar la seguridad y la privacidad de los intercambios electrónicos, se debe identificar al destinatario antes de darle acceso a la comunicación electrónica.

205. En el artículo 20 no se mencionan conceptos utilizados en textos anteriores de la CNUDMI, como "envío" y "recepción" (véase el art. 10 de la CCE), porque se redactó poniendo el énfasis en la equivalencia funcional entre los servicios de correo certificado y los servicios de entrega electrónica certificada, y no en los conceptos subyacentes.

Referencias

A/CN.9/971, párrs. 139 a 141; A/CN.9/1005, párrs. 62 a 64; A/CN.9/1045, párrs. 42 a 44.

9. Artículo 21. Autenticación de sitios web

206. El artículo 21 trata de la autenticación de sitios web, cuya función esencial es vincular un sitio web a la persona a quien se haya asignado el nombre de dominio o a quien se haya otorgado una licencia respecto de ese nombre, con el fin de confirmar la fiabilidad del sitio web. Por lo tanto, la autenticación de un sitio web comprende dos elementos: la identificación del titular del nombre de dominio del sitio web y la vinculación de esa persona al sitio web. La autenticación de un sitio web no tiene por objeto identificar ese sitio web.

207. El artículo 21 no es una norma de equivalencia funcional, ya que un sitio web existe solamente en forma electrónica y, por lo tanto, la autenticación de un sitio web no tiene un equivalente fuera de línea.

208. El término "titular del nombre de dominio" se refiere a la persona a quien un registrador de nombres de dominio ha asignado el nombre de dominio o ha otorgado una licencia para utilizarlo. Esa persona no tiene por qué ser el "propietario" del sitio web, ni el proveedor de contenidos, ni el operador.

209. Puede ser necesario adoptar medidas de protección adicionales en los casos en que se utilice un nombre de dominio para una plataforma que aloja páginas web creadas y administradas por distintas personas. Por ejemplo, el operador de la plataforma puede tener que identificar a las personas de acuerdo con un procedimiento determinado para poder mantener la autenticación del sitio web.

Referencias

A/CN.9/971, párrs. 142 a 144; A/CN.9/1005, párrs. 65 y 66; A/CN.9/1045, párrs. 47 y 48.

10. Artículo 22. Requisitos de fiabilidad de los servicios de confianza

210. En el artículo 22 figura una lista no taxativa de circunstancias que pueden ser pertinentes para determinar la fiabilidad del método utilizado de acuerdo con el criterio *ex post*. La lista se inspira en las listas que figuran en el artículo 10 de la LMFE y en el artículo 12 de la LMDTE.

211. Al igual que el concepto de método fiable utilizado en relación con los servicios de gestión de la identidad (véase el párr. 141 *supra*), la noción de método fiable utilizada para los servicios de confianza es relativa y varía en función del fin que se persiga. El carácter relativo de la fiabilidad se refleja en el párrafo 1 a), concretamente en las palabras "tan fiable como resulte apropiado" ―que, según una práctica bien establecida de la CNUDMI, pretenden reflejar mejor los diversos usos de los servicios de confianza― y en la referencia a "los fines para los que se utiliza el servicio de confianza".

Niveles de fiabilidad

212. En la LMFE y en varias leyes nacionales y regionales en materia de firmas electrónicas se distingue entre diversos servicios de confianza según el nivel de fiabilidad que ofrezcan. Concretamente, esas leyes atribuyen mayores efectos jurídicos a las firmas electrónicas que cumplen determinados requisitos, las que, por lo tanto, se considera que ofrecen un nivel de fiabilidad más alto. Además, es posible que algunas leyes solo permitan designar firmas electrónicas que ofrezcan un mayor nivel de fiabilidad. Ese criterio no se siguió en la Ley Modelo, que permite designar servicios de confianza independientemente del nivel de fiabilidad que ofrezcan.

213. Dado que las credenciales de identidad que ofrecen un alto nivel de garantía pueden utilizarse para servicios de confianza con diferentes niveles de fiabilidad, no existe una correlación directa entre el nivel de garantía de un servicio de gestión de la identidad y el nivel de fiabilidad de un servicio de confianza.

Referencias

A/CN.9/965, párr. 106; A/CN.9/971, párrs. 120 y 121; A/CN.9/1005, párrs. 67, 68 y 73; A/CN.9/1045, párrs. 18 a 21, 27 a 29, 52 a 57 y 61; A/CN.9/1051, párrs. 45 y 46; A/CN.9/1087, párrs. 87, 105 y 106.

11. Artículo 23. Designación de servicios de confianza fiables

214. El artículo 23 complementa el artículo 22 al permitir que se designen servicios de confianza de acuerdo con el criterio *ex ante*. Más concretamente, establece las condiciones que debe reunir un servicio de confianza para ser incluido en una lista de servicios de confianza designados cuya fiabilidad se presume a los efectos de los artículos 16 a 21.

215. El artículo 23 se centra en la designación de servicios de confianza en el entendimiento de que el proceso de designación de servicios de confianza implica necesariamente una evaluación de los métodos utilizados. Del mismo modo que la designación de servicios de gestión de la identidad, la designación de servicios de confianza que se presume que utilizan métodos fiables no se hace con respecto a tipos genéricos de servicios de confianza ni a todos los servicios de confianza ofrecidos por un determinado proveedor de servicios de confianza, sino más bien respecto de un servicio de confianza concreto, prestado por un proveedor de servicios identificado.

216. Dado que el único efecto jurídico de la designación es la presunción de fiabilidad del método utilizado, el uso de servicios de confianza que han sido designados, pero que han perdido esa designación, impide que la parte interesada se ampare en esa presunción, pero no tiene consecuencias en lo que respecta a la determinación *ex post* de la fiabilidad del método.

217. El artículo 23 exige que la autoridad designadora publique una lista de servicios de confianza designados, con detalles de los proveedores de esos servicios. La finalidad de esa obligación es promover la transparencia e informar a los posibles usuarios de servicios de confianza. Las jurisdicciones promulgantes podrían estudiar la forma de combinar esas listas para que la información pueda consultarse en un archivo supranacional centralizado, similar a algunos ejemplos regionales que ya existen.

Referencias

A/CN.9/971, párrs. 150 a 152; A/CN.9/1005, párrs. 69 a 73; A/CN.9/1045, párrs. 30 a 33 y 58 a 61.

12. Artículo 24. Responsabilidad de los proveedores de servicios de confianza

218. Como principio general, los proveedores de servicios de confianza deberían responder de las consecuencias de la falta de prestación de los servicios en la forma convenida o, en su defecto, conforme a lo exigido por la ley. Hay varios factores que son pertinentes para determinar la magnitud de esa responsabilidad, entre ellos el tipo de servicio de confianza prestado.

219. El artículo 24 está redactado de manera similar al artículo 12, que regula la responsabilidad de los proveedores de servicios de gestión de la identidad, por lo que las consideraciones realizadas en relación con el artículo 12 pueden aplicarse también al artículo 24. En particular, el artículo 24, al igual que el artículo 12, establece un fundamento legal de la responsabilidad que se aplica junto con la responsabilidad contractual y extracontractual, y la aplicación de las normas del derecho interno en materia de responsabilidad contractual y extracontractual que son pertinentes respecto de los proveedores de servicios de confianza no se ve afectada por el artículo 24, como se indica en el párrafo 2 a).

220. En algunos casos puede ser difícil o imposible identificar al proveedor de los servicios de confianza (p. ej., servicios de estampado de fecha y hora utilizados junto con la tecnología de registros distribuidos) y, por lo tanto, quizás no sea posible atribuir

responsabilidad. En esos casos, el sistema puede ofrecer otros medios de generar confianza en la utilización del servicio de confianza.

221. Entre los textos anteriores de la CNUDMI, la LMFE contiene disposiciones sobre las consecuencias jurídicas del proceder del firmante (art. 8), del prestador de servicios de certificación (art. 9) y de la parte que confía (art. 11). En esas disposiciones se establecen las obligaciones de cada una de las entidades que intervienen en el ciclo de vida de la firma electrónica. Además, la LMFE reconoce la posibilidad de que los prestadores de servicios de certificación limiten el alcance o la magnitud de su responsabilidad[30].

Referencias

A/CN.9/1005, párrs. 74 a 76; A/CN.9/1045, párrs. 62 a 66; A/CN.9/1087, párr. 89.

D. Capítulo IV. Aspectos internacionales (artículos 25 a 27)

1. Artículo 25. Reconocimiento transfronterizo de la identificación electrónica

222. El artículo 25 establece un mecanismo para el reconocimiento jurídico transfronterizo de la identificación electrónica que tiene por objeto conceder el mismo tratamiento jurídico a los sistemas y servicios de gestión de la identidad y las credenciales de identidad tanto nacionales como extranjeros. Se basa en el principio de no discriminación por razón del origen geográfico y se centra en la identificación electrónica como resultado de la utilización de sistemas y servicios de gestión de la identidad y credenciales de identidad.

223. Uno de los objetivos del artículo 25 es reducir la necesidad de que los proveedores de servicios soliciten la designación prevista en el artículo 23 en varias jurisdicciones. Esto puede ser especialmente útil en aquellas jurisdicciones que utilizan normas técnicas nacionales que, como tales, pueden no ser idénticas a las normas técnicas extranjeras. El reconocimiento recíproco de la certificación, en los lugares en que se dispone de ese servicio, puede desempeñar un papel importante en la aplicación de esta disposición.

224. Los niveles de fiabilidad definidos en diferentes jurisdicciones pueden no coincidir exactamente. La falta de coincidencia es una situación que probablemente se plantee debido a la inexistencia de definiciones de niveles de fiabilidad específicos acordadas universalmente. Para superar los obstáculos al reconocimiento transfronterizo que se derivan de esa falta de coincidencia, el artículo 25 hace referencia a “un nivel de fiabilidad que sea como mínimo equivalente”, noción que abarca niveles de fiabilidad iguales o superiores al exigido. No debe interpretarse que este concepto exige el cumplimiento de requisitos técnicos estrictos, que podrían obstaculizar el reconocimiento recíproco y, en última instancia, el comercio.

225. La referencia a “un sistema de gestión de la identidad, un servicio de gestión de la identidad o una credencial de identidad, según corresponda” pretende captar todos los aspectos que posiblemente sean pertinentes para el reconocimiento transfronterizo de la identificación electrónica. En la práctica, puede ser preferible centrar la atención en un determinado servicio de gestión de la identidad para evitar que se reconozcan como igualmente fiables todos los servicios de gestión de la identidad respaldados por un sistema de gestión de la identidad, aunque uno o más de esos servicios puedan ofrecer un nivel de fiabilidad inferior. Por otra parte, no deberían reconocerse credenciales de identidad que hubieran permanecido inalteradas a pesar de que el servicio de gestión de la identidad utilizado para emitirlas se haya visto comprometido.

226. A los efectos del reconocimiento de servicios y sistemas de gestión de la identidad extranjeros y de credenciales de identidad extranjeras puede ser necesario que el proveedor de servicios adapte sus condiciones de servicio. Por ejemplo, las normas

[30] En el documento *Fomento de la confianza en el comercio electrónico*, párrs. 211 a 232, puede verse un análisis de casos concretos de responsabilidad en el marco de una infraestructura de clave pública.

jurídicas imperativas de la jurisdicción que reconoce el servicio pueden afectar a la capacidad del proveedor de servicios de limitar su responsabilidad.

227. En el párrafo 3 se aclara además que las entidades designadoras pueden designar servicios de gestión de la identidad y de confianza extranjeros. Esta disposición amplía el mecanismo previsto en el artículo 11, párrafo 4, en el que se prohíbe la discriminación por motivos geográficos en el proceso de designación, al permitir que la entidad designadora de la jurisdicción promulgante se base en la designación realizada por una entidad designadora extranjera e incluir a los sistemas de gestión de la identidad y las credenciales de identidad como posibles objetos de designación. Por lo tanto, en el párrafo 3 se aplica el criterio *ex ante*.

228. Al determinar la equivalencia, la autoridad competente debería tener en cuenta la lista de circunstancias pertinentes para determinar la fiabilidad de los métodos utilizados en los servicios de gestión de la identidad mencionados en el artículo 10, párrafo 2, a fin de que haya coherencia entre las determinaciones de fiabilidad.

229. La determinación de la fiabilidad de un servicio de gestión de la identidad, un sistema de gestión de la identidad o una credencial de identidad es una tarea que requiere mucho tiempo y recursos, y tal vez no todas las jurisdicciones dispongan de recursos suficientes. Las jurisdicciones que tienen menos recursos pueden verse especialmente favorecidas por la posibilidad de reconocer servicios y sistemas de gestión de la identidad extranjeros y credenciales de identidad extranjeras basándose en las determinaciones y designaciones extranjeras. Los mecanismos basados en el párrafo 3 también pueden sustituir a los mecanismos basados en la celebración de acuerdos *ad hoc* de reconocimiento recíproco entre organismos de supervisión.

230. Al reglamentar la aplicación de estas disposiciones, la jurisdicción promulgante podrá decidir si el párrafo 3 se aplicará sobre la base del reconocimiento automático (p. ej., los servicios de gestión de la identidad designados por la entidad extranjera tendrían automáticamente la condición jurídica de designados en la jurisdicción promulgante), o si se establecerá una presunción (p. ej., los servicios de gestión de la identidad designados por la entidad extranjera se presumirían fiables en la jurisdicción promulgante, pero no tendrían la condición jurídica de designados en esa jurisdicción si no hubiera una intervención posterior de la entidad designadora).

Referencias

A/CN.9/936, párrs. 75 a 77; A/CN.9/1005, párr. 120; A/CN.9/1045, párrs. 67 a 74; A/CN.9/1051, párrs. 57 a 66; A/CN.9/1087, párrs. 90 y 101.

2. Artículo 26. Reconocimiento transfronterizo del resultado de la utilización de servicios de confianza

231. El artículo 26 introduce un mecanismo para el reconocimiento transfronterizo del resultado de la utilización de servicios de confianza, similar al establecido en el artículo 25 para la identificación electrónica. En consecuencia, las consideraciones realizadas en relación con el artículo 25 pueden aplicarse al artículo 26.

232. El artículo 26 es, en general, compatible con el empleo de los mecanismos existentes para el reconocimiento transfronterizo del resultado de la utilización de servicios de confianza, como el reconocimiento y la certificación recíprocos entre infraestructuras de clave pública[31].

Referencias

A/CN.9/1087, párrs. 90 a 101.

[31] Para más información sobre el reconocimiento recíproco y la certificación recíproca, véase *Fomento de la confianza en el comercio electrónico*, párrs. 163 a 172.

3. Artículo 27. Cooperación

233. Los mecanismos de cooperación institucional pueden contribuir considerablemente al logro del reconocimiento jurídico recíproco y la interoperabilidad técnica de los sistemas de gestión de la identidad y los servicios de confianza. Esos mecanismos existen en diferentes formas y pueden ser de carácter público o privado. La cooperación puede consistir en el intercambio de información, experiencia y buenas prácticas, en particular con respecto a los requisitos técnicos, entre ellos los niveles de garantía y los niveles de fiabilidad.

234. Además, el artículo 27 puede facilitar que se llegue a un acuerdo sobre definiciones comunes de las normas técnicas, incluidos los niveles de garantía y los niveles de fiabilidad, que sean de utilidad para determinar la equivalencia. En la práctica empresarial, los conceptos de nivel de garantía y de nivel de fiabilidad se utilizan como términos técnicos para evaluar la gestión de la identidad y los servicios de confianza, respectivamente. La Ley Modelo no establece un conjunto común de niveles de garantía para los sistemas de gestión de la identidad ni de niveles de fiabilidad para los servicios de confianza debido a las dificultades que existen para llegar a un acuerdo sobre definiciones aceptadas universalmente. Además, hay diferencias entre las jurisdicciones en cuanto a las leyes y prácticas empresariales que rigen la formulación de esas definiciones, en particular en lo que respecta a la función de las autoridades centrales por oposición al papel que corresponde a los contratos.

235. La cooperación debería ser voluntaria y ajustarse a las leyes y reglamentos nacionales aplicables. La referencia a las “entidades extranjeras” pretende abarcar a todas las entidades, cualquiera sea su naturaleza jurídica, que puedan contribuir al logro de los objetivos previstos.

Referencias

A/CN.9/965, párrs. 119 y 120; A/CN.9/1005, párr. 122; A/CN.9/1045, párr. 75; A/CN.9/WG.IV/WP.153, párrs. 95 a 98; A/CN.9/1087, párrs. 108 y 109.