Naciones Unidas A/CN.9/WG.IV/WP.160

Asamblea General

Distr. limitada
16 de septiembre de 2019
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
59º período de sesiones
Viena, 25 a 29 de noviembre de 2019

Proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza

Nota de la Secretaría

Índice

V.19-09433 (S) 071019 071019

I. Introducción

1. En la versión revisada del proyecto de disposiciones sobre la gestión de la identidad y los servicios de confianza que figura en el anexo del presente documento se reflejan las deliberaciones mantenidas por el Grupo de Trabajo en su 58º período de sesiones (Nueva York, 8 a 12 de abril de 2019), así como las conclusiones de las consultas celebradas por la Secretaría con especialistas en la materia conforme a la solicitud del Grupo de Trabajo (A/CN.9/971, párr. 67). Con este fin, la Secretaría organizó una reunión de expertos (Viena, 22 y 23 de julio de 2019) a fin de examinar los requisitos de normas y procedimientos que deben cumplir los sistemas de gestión de la identidad a efectos de su reconocimiento jurídico, así como otras cuestiones abordadas en el proyecto de disposiciones, en particular la fiabilidad de estos sistemas y las obligaciones y responsabilidades de los proveedores de servicios de gestión de la identidad.

2. En el documento A/CN.9/WG.IV/WP.159, párrs. 6 a 17, figura información de antecedentes sobre la labor que está llevando a cabo el Grupo de Trabajo IV.

Anexo I

Proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza

Capítulo I. Disposiciones generales

Artículo 1. Definiciones

A los efectos del presente [instrumento]:

a) Por “atributo” se entenderá un elemento de información o datos vinculados a un sujeto[1];

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

c) Por “identificación” se entenderá el proceso de reunión, verificación y validación de atributos que sean suficientes para definir y confirmar la identidad de un sujeto en un contexto en particular[2];

d) Por “identidad” se entenderá un conjunto de atributos que [permiten que un sujeto sea debidamente diferenciado] [describen a un sujeto [de manera inequívoca]] en un contexto dado[3];

e) Por “credenciales de identidad” se entenderá [un conjunto de datos que se presenta como prueba de la identidad declarada] [los datos o el objeto físico en que pueden residir los datos, que un sujeto puede presentar para verificar o autenticar su identidad en un contexto en línea][4, 5];

f) Por “servicios de gestión de la identidad” se entenderá los servicios que consisten en gestionar la identificación de sujetos en un contexto en línea;

g) Por “proveedor de servicios de gestión de la identidad” se entenderá la persona [que presta servicios relacionados con los sistemas de gestión de la identidad] [responsable de un sistema de gestión de la identidad][6, 7];

---

[1] Véase A/CN.9/WG.IV/WP.150, párr. 13.

[2] Véase A/CN.9/WG.IV/WP.150, párr. 29. El Grupo de Trabajo tal vez desee examinar si esta definición refleja fielmente el uso dado al término “identificación” en este proyecto de disposiciones (teniendo especialmente presentes las disposiciones del proyecto de artículo 9), o si convendría modificarla para que incluyera otros procesos de gestión de la identidad como la inscripción del sujeto en un sistema de gestión de la identidad y la emisión de credenciales de identidad.

[3] Véase A/CN.9/WG.IV/WP.150, párr. 38. Cuando examine la definición de “identidad”, el Grupo de Trabajo tal vez desee plantearse si el requisito de singularidad de los atributos es necesario a los efectos de la labor del Grupo de Trabajo, habida cuenta de que a) la singularidad es una cualidad de la identidad primaria (o básica), y b) la identidad primaria (o básica) está excluida actualmente del ámbito de su labor (A/CN.9/965, párr. 10).

[4] Esta definición es una adaptación de la que figura en el artículo 59.1-550 de la Ley de Gestión de la Identidad Electrónica de Virginia (título 59.1, capítulo 50, del Código de Virginia).

[5] Véase A/CN.9/WG.IV/WP.150, párr. 21. El término “credenciales de identidad” es, en sentido amplio, sinónimo del término “medios de identificación electrónica” que, en el artículo 3, párr. 2, del 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), se define como “una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea”.

[6] El Grupo de Trabajo ha convenido en que se utilice el término “proveedor de servicios de gestión de la identidad” en lugar de “operador del sistema de gestión de la identidad” (A/CN.9/971, párr. 97).

[7] El Grupo de Trabajo tal vez desee examinar si debería mantenerse esta definición en su forma actual, en vista de las definiciones del término “proveedor de identidad” que figuran en el párrafo 37 del documento A/CN.9/WG.IV/WP.150, a saber, a) una entidad encargada de la

h) Por “sistema de gestión de la identidad” se entenderá un conjunto de procesos para gestionar la identificación de sujetos en un contexto en línea[8];

i) Por “parte que confía” se entenderá toda persona que pueda actuar sobre la base de servicios de gestión de la identidad o servicios de confianza;

j) Por “sujeto” se entenderá la persona, o el objeto que sea identificado en un contexto en particular[9];

k) Por “servicio de confianza”[10] se entenderá un servicio electrónico que ofrezca cierto nivel de fiabilidad en cuanto a las propiedades de los datos;

l) Por “proveedor de servicios de confianza” se entenderá la persona que preste uno o más servicios de confianza.

Artículo 2. Ámbito de aplicación

El presente [instrumento] será aplicable a la utilización y el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza en el contexto de actividades comerciales[11] y servicios [públicos][12] relacionados con el comercio[13].

identificación de personas físicas, entidades jurídicas, dispositivos y objetos digitales, de la expedición de las credenciales de identidad correspondientes y del mantenimiento y la gestión de la información sobre la identidad de los distintos sujetos; y b) una entidad que crea, mantiene y gestiona información digna de confianza sobre la identidad de otras entidades (por ejemplo, usuarios/abonados, organizaciones y dispositivos) y ofrece servicios de identidad basados en relaciones de confianza, negocio y otros tipos de relaciones.

[8] Véase A/CN.9/WG.IV/WP.150, párr. 35. En el 57º período de sesiones del Grupo de Trabajo, se dijo que esa definición podría hacer pensar que era necesario mencionar conjuntamente la “identificación”, la “autenticación” y la “autorización”. Por tal motivo, se sostuvo que era preferible la definición de “identificación electrónica” recogida en el reglamento eIDAS (A/CN.9/965, párr. 91). El término “identificación electrónica” se define en el artículo 3, párrafo 1, del reglamento eIDAS, como “el proceso de utilizar los datos de identificación de una persona [es decir, las “credenciales de identidad”, tal como se definen en el presente documento] en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica”.

[9] Véase A/CN.9/WG.IV/WP.150, párr. 38.

[10] El Grupo de Trabajo tal vez desee plantearse si en inglés debería decirse “trusted service” (en lugar de “trust service”) para evitar cualquier ambigüedad en relación con el concepto jurídico firmemente establecido de “trust” en el sentido de “fideicomiso” (A/CN.9/965, párrs. 14 y 101).

[11] Conforme a lo acordado por el Grupo de Trabajo en su 58º período de sesiones, se ha reformulado esta disposición a fin de combinar elementos de las dos opciones que se presentaron en el artículo 1, párr. 1 del documento A/CN.9/WG.IV/WP.157 (A/CN.9/971, párr. 23). En su 52º período de sesiones, la Comisión señaló que, en esta etapa inicial del proyecto, la labor del Grupo de Trabajo debía encaminarse a elaborar un instrumento que pudiera aplicarse a la utilización de los sistemas de gestión de la identidad y los servicios de confianza tanto a nivel nacional como a través de fronteras (A/74/17, párr. 172). Esta posición se refleja en la referencia que en esta disposición se hace tanto a la “utilización” como al “reconocimiento” de los sistemas de gestión de la identidad y los servicios de confianza.

[12] El Grupo de Trabajo tal vez desee examinar si es necesario mencionar el calificativo “públicos” en la disposición o si bastaría con que en ella figurase una referencia genérica a los “servicios relacionados con el comercio” para abarcar todas las operaciones que, pese a no ser comerciales por naturaleza, son pertinentes para el comercio, como la interacción con los sistemas de ventanilla única para operaciones aduaneras.

[13] El Grupo de Trabajo ha acordado que en el instrumento se debe prever la posibilidad de utilizar el producto de la labor de la CNUDMI para necesidades fuera de los entornos puramente comerciales (A/CN.9/971, párr. 23). En su 52º período de sesiones, la Comisión observó que el resultado de esa labor repercutiría en aspectos que iban más allá de las operaciones comerciales (A/74/17, párr. 172).

Artículo 3. Utilización voluntaria de sistemas de gestión de la identidad y servicios de confianza[14]

1. Nada de lo dispuesto en el presente [instrumento] obligará a sujeto alguno a [utilizar un sistema de gestión de la identidad] [aceptar credenciales de identidad] ni a utilizar un servicio de confianza sin su consentimiento.

2. A los efectos de lo dispuesto en el párrafo 1, el consentimiento de un sujeto podrá inferirse de su conducta[15].

Artículo 4. Interpretación[16]

1. En la interpretación del presente [instrumento] se tendrán en cuenta su carácter 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 el presente [instrumento] que no estén expresamente resueltas en él se dirimirán de conformidad con los principios generales en que se basa este [instrumento], en particular la no discriminación contra el uso de medios electrónicos, la neutralidad tecnológica y la equivalencia funcional [y ...][17] [o, a falta de tales principios, de conformidad con la ley aplicable en virtud de las normas del derecho internacional privado][18].

Capítulo II. Gestión de la identidad

Artículo 5. Reconocimiento jurídico de un sistema de gestión de la identidad[19]

1. No se negarán efectos jurídicos, validez, fuerza ejecutoria ni admisibilidad como prueba a [la utilización de] [credenciales de identidad] [un sistema de gestión de la identidad] por la única razón de que:

a) [los resultados de la verificación[20] de la identidad estén] [el sistema de gestión de la identidad esté] en forma electrónica; o

b) el sistema de gestión de la identidad no sea uno cuya fiabilidad se hubiera establecido de conformidad con el artículo 11.

---

[14] El contenido del proyecto de artículo 2 del documento A/CN.9/WG.IV/WP.157, que trata de las "cuestiones no afectadas por este [proyecto de instrumento]" se incorpora en adelante a los proyectos de artículo 5 y 13. Del mismo modo, el Grupo de Trabajo tal vez desee considerar si convendría incorporar el contenido actual del proyecto de artículo 3 a los proyectos de artículo 5 y 13.

[15] Si el sujeto fuese un objeto físico o digital que no es capaz de tener una conducta autónoma, se tendrá en cuenta el consentimiento de la persona física o jurídica que sea legalmente responsable de dicho sujeto a los efectos de este artículo (A/CN.9/965, párr. 109).

[16] En su 58º período de sesiones, el Grupo de Trabajo no examinó una disposición sobre la interpretación del instrumento (proyecto de artículo 5 del documento A/CN.9/WG.IV/WP.157) que estaba basada en disposiciones similares de otros textos de la CNUDMI. El Grupo de Trabajo tal vez desee plantearse si convendría hacer referencia a la buena fe y, si así fuera, si cabría especificar "la buena fe en el comercio internacional".

[17] El Grupo de Trabajo tal vez desee examinar la pertinencia de enumerar también otros principios generales, en particular el principio de la transparencia (véase A/CN.9/936, párr. 88).

[18] La frase "o, a falta de tales principios, de conformidad con la ley aplicable en virtud de las normas del derecho internacional privado", que se añadió a esta disposición, puede resultar especialmente útil en el contexto transfronterizo.

[19] El párrafo 1 del proyecto de artículo 5 sigue la misma estructura que el proyecto de artículo 13, que a su vez refleja las deliberaciones mantenidas por el Grupo de Trabajo en su 58º período de sesiones. En esta disposición se establece la eficacia jurídica de la identificación que se realiza por medios electrónicos con independencia de que exista un procedimiento de identificación no electrónico. Los párrafos 2 a 4 se han formulado sobre la base del proyecto de artículo 2 del documento A/CN.9/WG.IV/WP.157.

[20] Si se mantiene la primera opción del apartado a), el Grupo de Trabajo tal vez desee examinar la posibilidad de añadir una referencia a la "autenticación" de la identidad, de conformidad con la definición de "credenciales de identidad" recogida en el artículo 1.

2. Nada de lo dispuesto en el presente [instrumento] obligará a persona alguna a identificar a un sujeto ni a utilizar un servicio de gestión de la identidad concreto.

3. Salvo en los casos previstos en el presente [instrumento], nada de lo dispuesto en [él] afectará a la aplicación a los servicios de gestión de la identidad de norma jurídica alguna [incluidas las normas jurídicas aplicables a la privacidad y la protección de datos][21].

4. Nada de lo dispuesto en el presente [instrumento] afectará a obligación legal alguna de identificar a un sujeto de conformidad con un procedimiento determinado que la ley establezca o exija[22].

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][23]:

a) inscribir a los sujetos, en particular mediante:

i) el registro y la reunión de los atributos de identidad;

ii) la realización de actividades de comprobación y verificación de la identidad; y

iii) la vinculación de las credenciales de identidad al sujeto;

b) actualizar los atributos;

c) administrar las credenciales de identidad de conformidad con las normas por las que se rija el sistema de gestión de la identidad, en particular mediante:

i) la emisión, entrega y activación de las credenciales;

ii) la suspensión, revocación y reactivación de las credenciales; y

iii) la renovación y sustitución de las credenciales;

d) autenticar a los sujetos, en particular mediante:

i) la gestión de los factores de autenticación; y

ii) la administración de los mecanismos de autenticación;

e) garantizar la disponibilidad en línea y el funcionamiento adecuado del sistema de gestión de la identidad; y

f) proporcionar un acceso razonable a las normas por las que se rija el sistema de gestión de la identidad[24].

[21] La referencia a la privacidad y la protección de datos pone de manifiesto la importancia que el Grupo de Trabajo asigna a estos temas, a la vez que reconoce que estos escapan a su mandato (A/CN.9/965, párr. 125).

[22] En esta nueva disposición se atiende a una preocupación planteada en el 52º período de sesiones del Grupo de Trabajo (A/CN.9/971, párr. 30).

[23] Estas obligaciones fundamentales de los proveedores de servicios de gestión de la identidad se determinaron con la ayuda de especialistas en la materia.

[24] El apartado f) se introdujo para reflejar el principio de la transparencia en la prestación de servicios de gestión de la identidad (véase también el proyecto de artículo 12, párr. 2 b)). En su 56º período de sesiones, el Grupo de Trabajo determinó que el principio de la transparencia era pertinente para las deliberaciones futuras sobre la gestión de la identidad (A/CN.9/936, párr. 88).

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

1. En caso de que se produjese una falla de seguridad o una pérdida de integridad que repercuta [de manera considerable] en el sistema de gestión de la identidad, en particular los atributos que se administran en él, el proveedor de servicios de gestión de la identidad deberá:

a) notificar inmediatamente [al órgano de supervisión] [a los sujetos y partes que confían que resulten afectados] la falla de seguridad o pérdida de integridad que se haya producido;

b) subsanar la falla de seguridad o la pérdida de integridad;

c) suspender las [credenciales de identidad] que resulten afectadas hasta que se subsane la falla de seguridad o la pérdida de integridad;

d) restablecer sin demora las [credenciales de identidad] que hayan resultado afectadas; y

e) revocar las [credenciales de identidad] que hayan resultado afectadas si la falla o la pérdida no puede subsanarse en un plazo de [plazo].

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

a) investigar la posible falla de seguridad o pérdida de integridad; y

b) adoptar cualquiera otra de las medidas previstas en el párrafo 1 que sea apropiada[25, 26].

Artículo 8. Obligaciones de los sujetos y las partes que confían

1. Todo sujeto deberá atenerse a las instrucciones razonables que comunique el proveedor de servicios de gestión de la identidad a fin de evitar la utilización no autorizada de las credenciales de identidad o los procesos de autenticación.

2. El sujeto deberá notificar al proveedor de servicios de gestión de la identidad en los siguientes casos:

a) cuando el sujeto tenga conocimiento de que las credenciales de identidad o los procesos de autenticación del correspondiente sistema de gestión de la identidad han quedado comprometidos; o

b) cuando las circunstancias de que tenga conocimiento el sujeto den lugar a un riesgo considerable de que las credenciales de identidad o los procesos de autenticación se hayan podido ver comprometidos.

3. Toda parte que confía deberá notificar al proveedor de servicios de gestión de la identidad en los siguientes casos:

a) cuando la parte que confía tenga conocimiento de que las credenciales de identidad o los procesos de autenticación del correspondiente sistema de gestión de la identidad hayan quedado comprometidos; o

b) cuando las circunstancias de que tenga conocimiento la parte que confía den lugar a un riesgo considerable de que las credenciales de identidad o los procesos de autenticación se hayan podido ver comprometidos.

[25] Por este párrafo se lleva a la práctica la propuesta de que en el proyecto de disposiciones se establezca la obligación de los proveedores de servicios de gestión de la identidad de tomar medidas en respuesta a las notificaciones de fallas de seguridad (A/CN.9/971, párr. 88).

[26] La disposición propuesta contiene texto opcional a fin de establecer un plazo dentro del cual deberá hacerse la notificación, indicar las partes a quienes habrá que notificar y determinar de qué magnitud deben ser los efectos en los servicios o los datos personales para que nazca la obligación de notificar.

Artículo 9. Identificación mediante sistemas de gestión de la identidad

Cuando la ley o una parte requiera que se identifique a un sujeto con arreglo a un determinado [método] [principio], ese requisito se dará por cumplido respecto de un sistema de gestión de la identidad si se utiliza un [método] [sistema de gestión de la identidad] fiable para identificar al sujeto[27, 28, 29].

Artículo 10. Factores pertinentes para la determinación de la fiabilidad[30]

1. En la determinación relativa a la fiabilidad del [método] [sistema de gestión de la identidad], deberán tenerse en cuenta todas las circunstancias pertinentes, por ejemplo:

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

b) el ajuste de las reglas de funcionamiento del sistema de gestión de la identidad a cualesquiera normas y procedimientos internacionales reconocidos, incluido el marco normativo relativo a los niveles de garantía, y en particular las reglas sobre:

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) las infraestructuras 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 sistema de gestión de la identidad; y

d) todo pacto que hubieran acordado las partes.

2. En la determinación relativa a la fiabilidad del [método] [sistema de gestión de la identidad], no se tomará en consideración:

a) el lugar en que funcione el sistema de gestión de la identidad; ni

---

[27] En esta disposición se refleja el proyecto de texto que acordó el Grupo de Trabajo en su 58º período de sesiones (A/CN.9/971, párr. 49). El Grupo de Trabajo tal vez desee plantearse si debería sustituirse la referencia a un “método fiable” por otra a un “sistema de gestión de la identidad fiable”.

[28] En el proyecto de instrumento, la utilización de un método (o un sistema de gestión de la identidad) fiable para la identificación es la piedra angular del régimen jurídico de reconocimiento de los sistemas de gestión de identidad. En este proyecto se prevén dos mecanismos para determinar la fiabilidad: por un lado, en su artículo 10 figura una lista indicativa de factores pertinentes para la determinación de la fiabilidad *ex post* y, por otro, en el artículo 11 se prevé el establecimiento de un mecanismo para la designación *ex ante* de métodos (o sistemas de gestión de la identidad) fiables. A raíz de consultas celebradas con especialistas, se ha suprimido la disposición relativa a la presunción de fiabilidad (proyecto de artículo 10 del documento A/CN.9/WG.IV/WP.157) a fin de simplificar el proyecto de instrumento. El contenido del párrafo 2 del proyecto de artículo 10 del documento A/CN.9/WG.IV/WP.157 se ha incorporado al proyecto de artículo 11, párrafo 5.

[29] El Grupo de Trabajo tal vez desee examinar si el proyecto de artículo 9 abarca los casos en que se debería establecer una equivalencia funcional entre la identificación en línea y fuera de línea. De no ser así, podría incluirse a tales efectos una nueva disposición con el siguiente texto u otro similar: “Cuando una norma jurídica requiera o permita la identificación de un sujeto, esa norma se dará por cumplida cuando se utilice un sistema de gestión de la identidad fiable”.

[30] El título de esta disposición refleja el acuerdo al que llegó el Grupo de Trabajo en su 58º período de sesiones (A/CN.9/971, párr. 59).

b) el lugar en que se encuentre el establecimiento del proveedor de servicios de gestión de la identidad[31].

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

1. [La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia] podrá decidir qué [métodos] [sistemas de gestión de la identidad] son fiables a los efectos del artículo 9[32, 33].

2. Toda designación que se realice con arreglo a lo dispuesto en el párrafo 1 deberá ajustarse a las normas y procedimientos internacionales reconocidos y pertinentes para determinar la fiabilidad de los sistemas de gestión de la identidad, en particular los marcos normativos relativos a los niveles de garantía[34, 35].

3. En la designación de [un método] [un sistema de gestión de la identidad], no se tomará en consideración:

a) el lugar en que funcione el sistema de gestión de la identidad; ni

b) el lugar en que se encuentre el establecimiento del proveedor de servicios de gestión de la identidad[36].

4. La identificación de un sujeto mediante credenciales de identidad emitidas por un sistema de gestión de la identidad cuya fiabilidad se haya establecido de conformidad con lo dispuesto en el párrafo 1 se reconocerá como una prueba fidedigna de la identidad del sujeto.

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

a) demuestre de cualquier otra manera la fiabilidad de [un método] [un sistema de gestión de la identidad] a los efectos del artículo 9; o

b) aduzca pruebas de que [un método] [un sistema de gestión de la identidad] cuya fiabilidad se hubiera establecido conforme a lo dispuesto en el párrafo 1 no es fiable.

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

1. Todo proveedor de servicios de gestión de la identidad que incumpla las obligaciones que le correspondan [como consecuencia de la prestación de servicios de gestión de la identidad] [en virtud del artículo 6] deberá responder de los daños y

---

[31] Se trata de una disposición de no discriminación geográfica basada en el artículo 12 de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (LMFE), que se pretende tenga por efecto permitir el reconocimiento transfronterizo de los sistemas de gestión de la identidad.

[32] Esta disposición se ha modificado para reflejar los cambios acordados por el Grupo de Trabajo en su 58º período de sesiones (A/CN.9/971, párr. 76), salvo el relativo a la introducción de una referencia al artículo 9 debido a los cambios que se hicieron en dicha disposición a raíz de consultas celebradas con especialistas. En su lugar, se introdujeron las palabras “son fiables a los efectos del artículo 9”.

[33] El Grupo de Trabajo tal vez desee examinar si en el instrumento debería abordarse la responsabilidad por daños que pudieran emerger de la utilización de un sistema cuya fiabilidad se hubiera establecido de conformidad con el proyecto de artículo 11.

[34] Esta disposición se ha modificado para reflejar los cambios acordados por el Grupo de Trabajo en su 58º período de sesiones (A/CN.9/971, párr. 76).

[35] El Grupo de Trabajo tal vez desee aclarar si los elementos que se enumeran en el proyecto de artículo 10 se aplican a la designación de un sistema de gestión de la identidad fiable con arreglo a lo dispuesto en el proyecto de artículo 11 (es decir, si la persona física o jurídica, el órgano o la entidad designadora debe tener en cuenta las circunstancias enumeradas en el artículo 10, párr. 1), y de ser así, de qué manera se aplican esos elementos a tal designación.

[36] Se trata de una disposición de no discriminación geográfica basada en el artículo 12 de la LMFE, que se pretende tenga por efecto permitir el reconocimiento transfronterizo de los sistemas de gestión de la identidad.

perjuicios que dicho incumplimiento cause deliberadamente o por negligencia a cualquier persona[37].

2. Sin perjuicio de lo dispuesto en el párrafo 1, el proveedor de servicios de gestión de la identidad no responderá de los daños que sean consecuencia de la utilización de un sistema de gestión de la identidad cuando:

a) esa utilización exceda las limitaciones establecidas [en cuanto a los fines o el valor de las operaciones para las que puede utilizarse el sistema de gestión de la identidad]; y

b) el proveedor de servicios de gestión de identidad haya proporcionado medios razonablemente accesibles que permitan [[al usuario[38] o] a un tercero][39] determinar cuáles son esas limitaciones[40].

3. Los proveedores de servicios de gestión de la identidad no responderán de los daños y perjuicios causados a una persona como consecuencia de la utilización de un sistema de gestión de la identidad cuya fiabilidad se hubiera establecido con arreglo a lo dispuesto en el artículo 11 si [la emisión de la credencial de identidad o la asignación de un atributo de identidad] se ajusta a:

a) las obligaciones que les incumben como consecuencia de la prestación de servicios de gestión de la identidad, en particular las que se enumeran en el artículo 6;

b) las reglas de funcionamiento del sistema de gestión de la identidad, en particular las que se enumeran en el artículo 10, párrafo 1 b); y

c) todo pacto que hubieran acordado las partes.

[4. El párrafo 3 no se aplicará a los casos en que el daño pueda atribuirse a un acto o una omisión del proveedor de servicios de gestión de la identidad que constituya [una negligencia grave o una conducta dolosa]][41].

---

[37] En esta disposición se refleja el proyecto de texto que acordó el Grupo de Trabajo en su 58º período de sesiones (A/CN.9/971, párr. 101). La disposición se enmendó nuevamente a fin de aclarar el motivo del daño por el cual se establece la responsabilidad.

[38] En caso de que se utilizase esta opción, el Grupo de Trabajo tal vez desee considerar la posibilidad de definir el término “usuario”.

[39] El Grupo de Trabajo tal vez desee examinar si convendría indicar en el proyecto de artículo las partes que deberían ser capaces de determinar las limitaciones y, de ser así, si esas partes deberían ser las mismas que aquellas ante las que pueden tener que responder los proveedores de servicios de gestión de la identidad.

[40] Esta disposición se basa en el art. 9, párr. 1 d), apartado ii), de la LMFE.

[41] Este párrafo reproduce el párrafo 4 del proyecto de artículo 13 del documento A/CN.9/WG.IV/WP.157. El Grupo de Trabajo tal vez desee examinar la posibilidad de suprimir el párrafo 4 en vista del párrafo 1.

Capítulo III. Servicios de confianza[42]

Artículo 13. Reconocimiento jurídico de servicios de confianza[43, 44]

1. No se negarán efectos jurídicos, validez ni fuerza ejecutoria [, ni admisibilidad como prueba][45] a [la información] [los datos][46] que se intercambien, verifiquen o autentiquen mediante la utilización o con el respaldo de un servicio de confianza [que cumpla los requisitos [del presente capítulo]], por la sola razón de que:

a) esa información se encuentre en forma electrónica; o

b) no esté respaldada por un servicio de confianza cuya fiabilidad se hubiera establecido de conformidad con el artículo 24.

2. Nada de lo dispuesto en el presente [instrumento] obligará a persona alguna a utilizar un servicio de confianza concreto[47].

3. Salvo en los casos previstos en el presente [instrumento], nada de lo dispuesto en [él] afectará a la aplicación a los servicios de confianza de norma jurídica alguna que se aplique a estos servicios [incluidas las normas jurídicas aplicables a la privacidad y la protección de datos][48].

Artículo 14. Obligaciones de los proveedores de servicios de confianza

1. Todo proveedor de servicios de confianza deberá garantizar la disponibilidad y el funcionamiento correcto de los servicios de confianza que preste.

---

[42] El capítulo sobre los servicios de confianza se ha revisado. En adelante, consta de una disposición general sobre el reconocimiento jurídico de los servicios de confianza (proyecto de artículo 13); una norma de fiabilidad general acompañada de una cláusula de no discriminación geográfica para facilitar el reconocimiento transfronterizo (proyecto de artículo 23); un mecanismo para la designación *ex ante* de servicios de confianza fiables (proyecto de artículo 24) y una lista de servicios de confianza (proyectos de artículo 16 a 22) que pueden utilizarse en forma de "módulos independientes" y también de manera combinada, a fin de ofrecer garantías respecto de ciertas propiedades de los datos. En particular, las firmas electrónicas guardan relación con el iniciador de los datos ("quién") y la intención perseguida por este con su creación ("por qué"); los sellos de tiempo electrónicos se refieren al momento en que tienen lugar ciertos acontecimientos relacionados con los datos ("cuándo"); una nueva disposición sobre la integridad aborda la garantía de que los datos no hayan sido modificados desde un momento determinado ("qué"); y los servicios de entrega están relacionados con la ubicación de los mensajes de datos en el ciberespacio ("dónde").

[43] Esta disposición se incorporó para reflejar el acuerdo al que llegó el Grupo de Trabajo en su 58º período de sesiones (A/CN.9/971, párrs. 112 a 115).

[44] El Grupo de Trabajo tal vez desee examinar si esta disposición de no discriminación debería centrarse en la información (o los datos) que se intercambia, verifica o autentica o, más bien, en el método utilizado para llevar a cabo las operaciones de verificación y autenticación. Un proyecto anterior de esta disposición, basado en el último de estos enfoques, tenía el siguiente tenor: "no se negarán efectos jurídicos, validez, fuerza ejecutoria ni admisibilidad como prueba a un servicio de confianza por la única razón de que se preste en forma electrónica" (artículo 6, párr. 2, del documento A/CN.9/WG.IV/WP.157).

[45] El Grupo de Trabajo tal vez desee considerar si convendría hacer referencia a "los datos" a fin de ajustar la disposición a la definición de "servicio de confianza".

[46] Se sugiere que se introduzcan las palabras "ni admisibilidad como prueba" a fin de ajustar esta disposición al proyecto de artículo 5.

[47] Los párrafos 2 y 3 se inspiraron en lo dispuesto en el proyecto de artículo 2 del documento A/CN.9/WG.IV/WP.157.

[48] La referencia a la privacidad y la protección de datos pone de manifiesto la importancia que el Grupo de Trabajo asigna a estos temas, a la vez que reconoce que estos escapan a su mandato (A/CN.9/965, párr. 125).

2. En caso de que se produjese una falla de seguridad o una pérdida de integridad que repercuta [de manera considerable] en los servicios de confianza, el proveedor de estos servicios deberá:

a) suspender la prestación de los servicios afectados [hasta [que se contenga la falla o la pérdida o se instituya un nuevo proceso de certificación u otro proceso similar]]; y

b) subsanar la falla de seguridad o la pérdida de integridad.

3. Todo proveedor de servicios de confianza deberá notificar sin demora [y, en todo caso, dentro de los [...] días siguientes a la fecha en que haya tomado conocimiento de ello,] [al órgano de supervisión] [a sus clientes[49] y partes que confían que resulten afectados] cualquier falla de seguridad o pérdida de integridad que repercuta [de manera considerable] en los servicios de confianza prestados o los datos personales guardados en ellos[50, 51].

Artículo 15. Obligaciones de los usuarios de servicios de confianza en caso de violación de los datos

Todo usuario[52] de un servicio de confianza deberá notificar al proveedor de dicho servicio cuando:

a) los datos de creación del servicio de confianza hayan quedado comprometidos; o

b) las circunstancias de que tenga conocimiento el usuario den lugar a un riesgo considerable de que los datos de creación del servicio de confianza se hayan podido ver comprometidos.

Artículo 16. Firmas electrónicas

Cuando una norma jurídica requiera o permita la firma [de una persona] [de un sujeto], esa norma se dará por cumplida [en relación con un mensaje de datos] cuando se utilice un método[53] fiable para:

a) identificar a la persona; o

b) indicar la voluntad que tiene esa persona respecto de la información contenida en el mensaje de datos[54].

---

[49] El Grupo de Trabajo tal vez desee considerar la posibilidad de definir el concepto de “cliente”.

[50] Este párrafo reproduce el párrafo 2 del proyecto de artículo 17 del documento A/CN.9/WG.IV/WP.157. El Grupo de Trabajo tal vez desee estudiar la posibilidad de suprimir la obligación que figura en ese párrafo e incorporarla como letra c) del párrafo 2, en consonancia con el proyecto de artículo 7.

[51] La disposición propuesta contiene texto opcional a fin de establecer un plazo dentro del cual deberá hacerse la notificación, indicar las partes a quienes habrá que notificar y determinar de qué magnitud deben ser los efectos en los servicios o los datos personales para que surja la obligación de notificar.

[52] El Grupo de Trabajo tal vez desee considerar la posibilidad de definir el término “usuario”.

[53] Siguiendo un enfoque similar al que se aplicó a la evaluación de la fiabilidad de los sistemas de gestión de la identidad, en el proyecto de disposiciones se prevén dos mecanismos para determinar la fiabilidad de un servicio de confianza: por un lado, en su artículo 23 figura una lista indicativa de factores pertinentes para la determinación de la fiabilidad *ex post* y, por otro, en el artículo 24 se prevé el establecimiento de un mecanismo para la designación *ex ante* de servicios de confianza fiables. Siguiendo también un enfoque similar al que se aplicó a los sistemas de gestión de la identidad, se ha suprimido la disposición relativa a la presunción de fiabilidad (proyecto de artículo 15 del documento A/CN.9/WG.IV/WP.157) a fin de simplificar el proyecto de instrumento. El contenido del párrafo 2 del proyecto de artículo 15 del documento A/CN.9/WG.IV/WP.157 se ha incorporado al proyecto de artículo 24, párrafo 5.

[54] En el 58º período de sesiones se sugirió que se añadieran las palabras “de manera que un tercero pueda verificar posteriormente esa voluntad” a fin de contemplar la función de “perpetuación” de las firmas electrónicas (de manera que un tercero pueda verificar posteriormente esa voluntad, véase el documento A/CN.9/971, párr. 122). También se sugirió que la posibilidad de realizar una

Artículo 17. Sellos electrónicos[55]

Cuando una norma jurídica requiera o permita que una persona estampe un sello, esa norma se dará por cumplida [en relación con un mensaje de datos] cuando se utilice un método fiable para:

a) identificar a la persona; y

b) detectar cualquier alteración del mensaje de datos desde su fecha de estampado.

Artículo 18. Sellos de tiempo electrónicos

Cuando una norma jurídica requiera o permita que [determinados documentos, registros, información o datos[56]] se vinculen a una fecha y una hora, esa norma se dará por cumplida [en relación con un mensaje de datos] cuando se utilice un método fiable para:

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

b) vincular dicha fecha y hora al mensaje de datos[57].

Artículo 19. Garantía de integridad[58]

Cuando una norma jurídica requiera o permita que se garantice la integridad de [un documento, un registro, información o datos], [ya sea mediante la conservación del documento en su forma original, su archivado u otro método,] esa norma se dará por cumplida en relación con un mensaje de datos cuando se utilice un método fiable para detectar las alteraciones del mensaje de datos desde su creación, distintas de la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación[59].

Artículo 20. Archivado electrónico[60]

Cuando una norma jurídica requiera o permita la conservación de [determinados documentos, registros o información], ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:

a) que sea posible acceder a la información contenida en ellos de manera que pueda consultarse posteriormente;

---

verificación posterior era una cualidad imprescindible de las firmas, de modo que no era necesario agregar la frase propuesta (*ibid.*).

[55] La presente disposición refleja el acuerdo al que llegó el Grupo de Trabajo de que se insertara una disposición independiente sobre los sellos electrónicos (A/CN.9/971, párr. 128). Siguiendo el enfoque simplificado que se explicó en la nota 42 de pie de página, el Grupo de Trabajo tal vez desee examinar si es necesario incorporar una disposición independiente o si es posible conseguir la misma función que se pretende que cumpla la utilización de los sellos electrónicos utilizando las firmas electrónicas (con respecto de la identificación) y la garantía de integridad (con respecto de la detección de alteraciones).

[56] La introducción de la palabra “datos” refleja el acuerdo al que llegó el Grupo de Trabajo (A/CN.9/971, párr. 130).

[57] La introducción de las palabras “y especificar el huso horario” refleja el acuerdo al que llegó el Grupo de Trabajo (A/CN.9/971, párr. 132).

[58] Esta disposición se ha incorporado a fin de introducir una norma general sobre la integridad de los mensajes de datos que ofrece el equivalente funcional del concepto de “original” utilizado en el contexto de las comunicaciones en soporte papel. Se presenta al Grupo de Trabajo en forma de alternativa al artículo 20 sobre el archivado electrónico. En la formulación actual de la norma, se establece claramente el servicio de confianza (ya que en ella se prevé la utilización de un método fiable para detectar las alteraciones).

[59] El Grupo de Trabajo tal vez desee examinar la posibilidad de incluir la obligación de que “se pueda acceder a la información recogida en el mensaje de datos de manera que pueda consultarse posteriormente” (véase también el proyecto de artículo 20 a)).

[60] Si se mantiene el proyecto de artículo 19, el Grupo de Trabajo tal vez desee examinar la conveniencia de suprimir el proyecto de artículo 20, por ser redundante.

b) que el mensaje de datos se conserve:

i) con el formato en que se haya generado, enviado o recibido; o

ii) con algún formato que pueda demostrarse que reproduce con exactitud la información generada, enviada o recibida; y

c) que se conserve, de haberla, 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[61].

Artículo 21. Servicios de entrega electrónica certificada

Cuando una norma jurídica requiera o permita que se demuestre el envío o la recepción de [un determinado documento, registro o información], esta norma se dará por cumplida [en relación con un mensaje de datos] si se utiliza un método fiable para garantizar que el mensaje de datos salió de un sistema de información o entró en dicho sistema[62].

Artículo 22. Autenticación de sitios web[63]

Cuando una norma jurídica requiera o permita la identificación del propietario de un sitio web, esa norma se dará por cumplida si se utiliza un método fiable para determinar la identidad de la persona que es propietaria de ese sitio web y para vincular esa persona al sitio web correspondiente.

Artículo 23. Norma de fiabilidad para los servicios de confianza[64]

1. A los efectos de lo dispuesto en los artículos [16 a 22], el método mencionado deberá:

a) ser tan fiable como sea apropiado para cumplir la función para la cual se utiliza, atendidas todas las circunstancias del caso, que pueden ser:

i) cualquier norma operacional por la que se rija el servicio de confianza;

ii) cualquier norma aplicable del sector;

iii) la seguridad de los equipos y programas informáticos;

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

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

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

vii) cualquier acuerdo pertinente; o

b) demostrar en la práctica que ha cumplido las funciones a las que se refiere el servicio de confianza correspondiente.

---

[61] Esta condición no es aplicable a la información que tenga por única finalidad permitir el envío o la recepción del mensaje; véase el art. 10, párr. 2, de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

[62] El texto refleja el acuerdo al que llegó el Grupo de Trabajo de que en el proyecto de disposición se incorporasen elementos del artículo 10 de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (A/CN.9/971, párr. 141).

[63] Siguiendo el enfoque simplificado que se explicó en la nota 42 de pie de página, el Grupo de Trabajo tal vez desee examinar si se pueden conseguir las funciones que se pretende que cumpla la autenticación de sitios web mediante la identificación de objetos digitales, incluidos los sitios web, con firmas electrónicas.

[64] Los elementos que se enumeran en el párrafo 1 a) se inspiraron en el artículo 10 de la LMFE y el artículo 12 a) de la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos, en que se establece una norma de fiabilidad general para el método utilizado.

2. En la determinación relativa a la fiabilidad del método a los efectos de lo dispuesto en los artículos [16 a 22], no se tomará en consideración:

a) el lugar desde el que se presta el servicio de confianza correspondiente; ni

b) el lugar en que se encuentre el establecimiento del proveedor de ese servicio[65].

Artículo 24. Designación de servicios de confianza fiables[66, 67]

1. [La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia] podrá decidir qué [métodos] [servicios de confianza] son fiables a los efectos de los artículos [16 a 22].

2. Toda designación que se realice con arreglo a lo dispuesto en el párrafo 1 deberá ajustarse a las normas y procedimientos internacionales reconocidos y pertinentes en materia de determinación de la fiabilidad de los servicios de confianza, en particular los marcos normativos relativos a los niveles de fiabilidad[68].

3. En la designación de [un método] [un servicio de confianza], no se tomará en consideración:

a) el lugar donde se preste el servicio de confianza correspondiente; ni

b) el lugar en que se encuentre el establecimiento del proveedor de ese servicio[69].

4. La utilización de un servicio de confianza cuya fiabilidad se haya establecido con arreglo a lo dispuesto en el párrafo 1 se considerará una prueba fidedigna de [la calidad de los datos a que se refiere ese servicio].

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

a) establezca de cualquier otra manera la fiabilidad de [un método] [un servicio de confianza] a los efectos de los artículos [16 a 22]; o

b) aduzca pruebas de que [un método] [un servicio de confianza] cuya fiabilidad se hubiera establecido conforme a lo dispuesto en el párrafo 1 no es fiable.

Artículo 25. Responsabilidad de los proveedores de servicios de confianza

1. Todo proveedor de servicios de confianza que incumpla las obligaciones que le correspondan [como consecuencia de la prestación de servicios de confianza] [en virtud [del artículo 14] [de este instrumento]] deberá responder de los daños y perjuicios que dicho incumplimiento cause deliberadamente o por negligencia a cualquier persona.

2. Sin perjuicio de lo dispuesto en el párrafo 1, el proveedor de servicios de confianza no responderá de los daños que sean consecuencia de la utilización de servicios de confianza cuando:

a) esa utilización exceda las limitaciones establecidas [en cuanto a los fines o el valor de las operaciones para las que puede utilizarse el servicio de confianza]; y

---

[65] Se trata de una disposición de no discriminación geográfica basada en el artículo 12 de la LMFE, cuyo efecto previsto es permitir el reconocimiento transfronterizo de los servicios de confianza.

[66] En esta disposición se prevé la posibilidad de realizar una evaluación *ex ante* de la fiabilidad de los servicios de confianza.

[67] El Grupo de Trabajo tal vez desee aclarar si los elementos que se enumeran en el proyecto de artículo 23 se aplican a la designación de un servicio de confianza fiable con arreglo a lo dispuesto en el proyecto de artículo 24 (es decir, si la persona física o jurídica, el órgano o la entidad designadora debe tener en cuenta las circunstancias enumeradas en el artículo 23, párr. 1 a), y de ser así, de qué manera se aplican esos elementos a tal designación.

[68] Esta disposición se ha modificado para reflejar los cambios acordados por el Grupo de Trabajo en su 58º período de sesiones (A/CN.9/971, párr. 76).

[69] Se trata de una disposición de no discriminación geográfica basada en el artículo 12 de la LMFE, cuyo efecto previsto es permitir el reconocimiento transfronterizo de los servicios de confianza.

b) el proveedor de servicios de confianza haya proporcionado medios razonablemente accesibles que permitan [[al usuario[70] o] a un tercero][71] determinar cuáles son esas limitaciones[72].

Capítulo IV. Aspectos internacionales

Artículo 26. Reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza[73]

1. Cuando [el funcionamiento de un sistema de gestión de la identidad] [la emisión de credenciales de identidad] o la prestación de un servicio de confianza tenga lugar fuera [de la jurisdicción promulgante], [dicho sistema] [dichas credenciales] o dicho servicio producirá[n] en [la jurisdicción promulgante] los mismos efectos jurídicos que produciría [un sistema de gestión de la identidad que funcionara] [una credencial de identidad que fuese emitida] en [la jurisdicción promulgante] o un servicio de confianza prestado en [dicha jurisdicción promulgante], siempre que ofrezca[n] [el mismo nivel de fiabilidad] [un nivel de fiabilidad sustancialmente equivalente][74, 75].

2. Para determinar si [unas credenciales de identidad] [un sistema de gestión de la identidad] o un servicio de confianza ofrece[n] [un] [el mismo] nivel de fiabilidad [sustancialmente equivalente], se tomarán en consideración [las normas internacionales reconocidas].

Artículo 27. Cooperación

[La persona, el órgano o la entidad, ya sea del sector público o del privado, especificado por el Estado promulgante] [deberá] [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 en lo que respecta a:

a) la certificación de los sistemas de gestión de la identidad y los servicios de confianza; y

b) 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.

---

[70] En caso de que se utilizase esta opción, el Grupo de Trabajo tal vez desee considerar la posibilidad de definir el término “usuario”.

[71] El Grupo de Trabajo tal vez desee examinar si convendría indicar en el proyecto de artículo las partes que deberían ser capaces de determinar las limitaciones y, de ser así, si esas partes deberían ser las mismas que aquellas ante las que pueden tener que responder los proveedores de servicios de confianza.

[72] Esta disposición se basa en el art. 9, párr. 1 d), apartado ii) de la LMFE.

[73] En esta disposición se reproducen los párrafos 2 y 3 del proyecto de artículo 19 del documento A/CN.9/WG.IV/WP.157. El Grupo de Trabajo tal vez desee examinar si debería mantenerse esta disposición en vista de los párrafos relativos a la no discriminación geográfica introducidos en los artículos 10, 11, 23 y 24.

[74] Esta disposición se inspira en el artículo 12, párr. 2, de la LMFE. Por consiguiente, el término “nivel de fiabilidad”, en la forma en que se utiliza en este proyecto de disposición, no tiene necesariamente el mismo significado que el que recibe en otros proyectos de disposición del instrumento.

[75] El Grupo de Trabajo tal vez desee examinar si esta disposición implica que todas las disposiciones legales de la jurisdicción promulgante se aplican al sistema de gestión de la identidad o servicio de confianza extranjero, en particular las disposiciones del presente instrumento y las disposiciones legales o contractuales sobre limitación de la responsabilidad.