Naciones Unidas A/CN.9/WG.IV/WP.163

Asamblea General

Distr. limitada
20 de febrero de 2020
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
60º período de sesiones
Nueva York, 6 a 9 de abril de 2020

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

Comunicación del Banco Mundial

Nota de la Secretaría

El Banco Mundial presentó un documento para que se examinara en el 60º período de sesiones del Grupo de Trabajo. En el anexo figura la traducción al español del texto en inglés que recibió la Secretaría.

V.20-01485 (S) 160320 160320

Anexo

Observaciones del Banco Mundial sobre el documento de trabajo A/CN.9/WG.IV/WP.162

El Banco Mundial se complace en presentar las siguientes observaciones sobre el documento A/CN.9/WG.IV/WP.162, “Proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza” (en lo sucesivo, “el proyecto de disposiciones”), con vistas al período de sesiones del Grupo de Trabajo IV que se celebrará en Nueva York del 6 al 9 de abril de 2020.

I. Comentarios y observaciones generales

1. Acento en la gestión de la identidad: En general, el Banco Mundial apoya la labor del Grupo de Trabajo IV, en particular en lo que respecta a la gestión de la identidad. Dado que la gestión de la identidad es el aspecto que más interesa al Banco Mundial, las siguientes observaciones se centran en las secciones del proyecto de disposiciones en que se trata esa cuestión.

2. Sistemas de gestión de la identidad frente a operaciones de identidad: El proyecto de disposiciones se centra principalmente en los sistemas de gestión de la identidad y en los proveedores de servicios de gestión de la identidad, y no tanto en las operaciones de identidad. Debido a la importancia de las operaciones de identidad, en particular desde el punto de vista del cumplimiento de las normas legales y el reconocimiento jurídico, y habida cuenta de que las operaciones de identidad electrónicas pueden y suelen llevarse a cabo sin utilizar sistemas de gestión de la identidad ni proveedores de servicios de gestión de la identidad, el Grupo de Trabajo debería considerar la posibilidad de examinar en mayor profundidad algunas cuestiones relativas a las operaciones de identidad.

3. Papeles: El proyecto de disposiciones se centra principalmente en la regulación de los sistemas de gestión de la identidad y los proveedores de servicios de gestión de la identidad y, a excepción de los artículos 5 y 8, no trata a fondo las necesidades de las partes que confían, los sujetos u otros posibles participantes en un sistema de gestión de la identidad o en una operación de identidad. Por ejemplo, en el proyecto de disposiciones no se trata la cuestión del derecho de la parte que confía a utilizar a un tercero para verificar la identidad cuando la ley exige que la parte que confía verifique la identidad. Al igual que ocurre con la cuestión de las operaciones de identidad, el Grupo de Trabajo debería considerar la posibilidad de dedicar mayor atención a las cuestiones que afectan a todos los papeles de los sistemas de gestión de la identidad, no solo al de proveedor de servicios de gestión de la identidad.

4. Relación entre los sistemas de gestión de la identidad del sector público y del sector privado: El proyecto de disposiciones se centra en los sistemas de gestión de la identidad del sector privado y en los proveedores de servicios de gestión de la identidad del sector privado. A primera vista, el proyecto de disposiciones no se aplicaría ni a los sistemas de gestión de la identidad ni a los proveedores de servicios de gestión de la identidad del sector público, como los sistemas nacionales de gestión de la identidad. Por consiguiente, dado que muchos de los sistemas nacionales de gestión de la identidad son sistemas gestionados por los Estados (por ejemplo, Estonia o la India), estos quedarían fuera del ámbito de aplicación del producto final del proyecto de disposiciones.

No obstante, es importante tener presente que es probable que la interacción entre los sistemas de gestión de la identidad de los sectores público y privado sea considerable. Por ejemplo, cabe suponer que el proyecto de disposiciones se aplicará en los casos en que un organismo público (por ejemplo, una parte que confía o un sujeto de datos) sea cliente de un proveedor de servicios de gestión de la identidad del sector privado, o utilice un sistema de identidad federado del sector privado en lugar de un sistema de

gestión de la identidad gestionado por un Estado. Además, los procesos de comprobación de identidad y autenticación utilizados por los proveedores de servicios de gestión de la identidad del sector privado se basan con frecuencia en las credenciales de identidad primaria emitidas por los sistemas del sector público, que suelen considerarse dignos de confianza y altamente fiables.

Por consiguiente, el Grupo de Trabajo debería examinar y aclarar la naturaleza de la relación entre los sistemas de gestión de la identidad de los sectores público y privado, entre otras cosas para determinar en qué casos sería apropiado que los sistemas de gestión de la identidad del sector privado aprovechasen la información relativa a la identidad primaria y los procesos de autenticación proporcionados por los Estados, o cuál sería el modo más indicado de hacerlo. Esto podría suponer, por ejemplo, examinar las normas relativas a:

- la utilización por los sistemas de gestión de la identidad del sector privado de números de identidad emitidos por el Estado u otra información de identificación;
- la utilización por los sistemas de gestión de la identidad del sector privado de credenciales de identidad emitidas por el Estado;
- el acceso por los sistemas de gestión de la identidad del sector privado a bases de datos estatales a efectos de comprobación de identidad y autenticación; o
- la utilización por los sistemas de gestión de la identidad del sector privado de información o procesos facilitados por las autoridades públicas, en general.

5. Marcos de confianza: En el proyecto de disposiciones no se trata la cuestión del papel de las normas contractuales que rigen los sistemas de gestión de la identidad individuales, lo que a menudo se denomina “marcos de confianza” o “normas del sistema” o “reglas del sistema” (que en lo sucesivo se denominarán colectivamente “marcos de confianza”), y cómo interactúan con el proyecto de disposiciones[1]. El Grupo de Trabajo debería considerar la posibilidad de volver a examinar el proyecto de disposiciones para aclarar la interacción entre el proyecto y los marcos de confianza de los sistemas de gestión de la identidad, así como qué cuestiones deberían tratarse en el proyecto de disposiciones, y con qué grado de detalle, en lugar de en los marcos de confianza de sistemas de gestión de la identidad individuales. Por ejemplo, algunas cuestiones como las obligaciones de los participantes, la fiabilidad y los niveles de garantía se suelen tratan en el marco de confianza específico de un sistema de gestión de la identidad individual.

Asimismo, el Grupo de Trabajo debería considerar la posibilidad de estudiar en qué medida las disposiciones de un marco de confianza pueden modificar o anular las del proyecto de disposiciones. Por ejemplo, con independencia de lo dispuesto en el proyecto de disposiciones con respecto a la responsabilidad, no está claro si las partes pueden definir sus propias normas sobre responsabilidad en el marco de confianza específico de su sistema de gestión de la identidad.

6. Utilización de los modelos legislativos relativos a las firmas electrónicas: La estructura y los criterios adoptados en el proyecto de disposiciones se basan en gran medida en la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas y, por consiguiente, no se tiene en consideración el hecho de que las cuestiones que se refieren a las firmas son muy diferentes de las que se han de tener presentes al abordar la identidad (si bien la identidad es, en ocasiones, un componente de la firma). Así pues, si bien es posible definir en la ley un único equivalente electrónico de los requisitos de firma, no resulta fácil hacer lo propio en lo que respecta a los requisitos para verificar la identidad.

[1] Si bien la expresión “reglas de funcionamiento del sistema de gestión de la identidad” aparece en los artículos 6 c), 6 f), 10, párr. 1 b), y 23, párr. 1 a), del proyecto de disposiciones, esta nunca se define ni se examina en detalle.

Parte del problema reside en el hecho de que las leyes que exigen una firma siempre exigen lo mismo (es decir, una firma), mientras que las leyes que exigen la identificación de una persona a menudo definen diferentes requisitos de diversa índole que debe cumplir el proceso de identificación en función de si la identidad es "primaria" o "funcional"[2], la finalidad con que se exige la identificación, el riesgo inherente, etc. En consecuencia, si bien es relativamente sencillo definir un equivalente jurídico al concepto unitario de firma, eso no significa necesariamente que se pueda proceder de igual modo en lo que respecta a los diversos criterios jurídicos aplicables a la identificación. Así pues, es importante que, en lugar de ceñirse a una estructura predeterminada basada en la Ley Modelo sobre las Firmas Electrónicas, el Grupo de Trabajo examine de manera independiente las cuestiones jurídicas que es preciso tener en cuenta en relación con la identidad.

7. Opciones de verificación de la identidad: La parte que confía dispone de dos opciones para verificar la identidad de la persona con la que está tratando, a saber, la parte que confía puede:

- efectuar la verificación de la identidad por sí misma, o bien
- recurrir a los servicios de gestión de la identidad prestados por un tercero.

La mayoría de las partes que confían optan por lo primero. No obstante, el proyecto de disposiciones se centra únicamente en la segunda opción. El Grupo de Trabajo podría tal vez considerar si el proyecto de disposiciones debería adoptar un enfoque más amplio del tema de la identidad y abordar las cuestiones que se plantean en ambas situaciones.

8. Derecho de la parte que confía a confiar: Lo ideal sería que el proyecto de disposiciones abordarse las cuestiones relativas al derecho de la parte que confía a confiar, entre las que figurarían, por ejemplo, el derecho de la parte que confía a lo siguiente: i) confiar en general en unas credenciales de identidad; ii) confiar en las credenciales de una tercera parte para satisfacer las requisitos específicos establecidos en una determinada ley que imponga la obligación de identificar; y iii) utilizar los servicios de gestión de la identidad prestados por un tercero para satisfacer su obligación de identificar a alguien.

9. Derecho de la parte que confía a utilizar a terceros: En relación con lo anterior, si bien algunas de las leyes que imponen la obligación de identificar autorizan expresamente la utilización de terceros proveedores de servicios (por ejemplo, el Reglamento de la Ley de Privacidad de los Consumidores de California)[3], muchas leyes no se pronuncian al respecto (u obligan a las partes que confían a efectuar la identificación). El Grupo de Trabajo también debería examinar estas cuestiones relacionadas con la identidad.

II. Observaciones artículo por artículo

1. Artículo 1. Definiciones

a) **Términos que faltan**: Hay varios términos que se utilizan en todo el proyecto de disposiciones, pero que no se definen. Los términos que se utilizan, pero no se definen son los siguientes:

- "factores de identificación electrónica", véase el artículo 6 d) i)
- "mecanismos de identificación electrónica", véanse los artículos 6 d) ii), 8 a), 8 b)

[2] Véanse, por ejemplo, las páginas 12 y 13 (entre otras) de la guía para profesionales publicada por el Banco Mundial en 2019, que puede consultarse en la siguiente dirección: https://id4d.worldbank.org/guide.

[3] Véase, Reglamento de la Ley de Privacidad de los Consumidores de California, artículo 4, sección 999.323 b). Puede consultarse en www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?

- “gestión de la identidad”, se utiliza como modificador en todo el documento, pero no se define
- “identificador”, véase el artículo 1 b)
- “normas por las que se rija el sistema de gestión de la identidad", véanse los artículos 6 c), 6 f), 10 b) y 23 a)
    - Es posible que ese término se refiera al marco de confianza de un sistema de gestión de la identidad individual, pero tal como está redactado podría aplicarse a cualquier ley o reglamento que rija el sistema de gestión de la identidad. Se debería aclarar en qué sentido se utiliza.
- “verificación”, véase el artículo 6 a) ii)
    - También convendría aclarar el concepto de “verificación”, ya que este término suele causar mucha confusión. Por ejemplo, el término “verificación de la identidad” se refiere frecuentemente a la identificación del sujeto de los datos, y en otros a la autenticación del sujeto de los datos. Habida cuenta de la frecuencia con que se utiliza este término, tendría que aclararse detalladamente y utilizarse de manera adecuada en todo el documento.

b) **Autenticación**: Los términos “autenticación” e “identificación electrónica” se utilizan básicamente con el mismo significado, si bien “autenticación” se utiliza en el contexto de los servicios de confianza e “identificación electrónica” se utiliza en el contexto de los servicios de gestión de la identidad. Dado que esos conceptos son idénticos, el Grupo de Trabajo podría considerar la posibilidad de utilizar el mismo término en ambos casos.

c) **Identificación electrónica**: La sustitución del término simple “identificación” por los términos compuestos “comprobación de identidad” e “identificación electrónica” es un paso importante para aclarar y distinguir dos aspectos del proceso de identidad. No obstante, podría suscitar preocupación la posibilidad de que el término “identificación electrónica” describa o se pueda confundir fácilmente con la totalidad del proceso de comprobación de identidad, emisión de credenciales y autenticación de la relación entre los datos de las credenciales y una persona. Así pues, se recomienda que el Grupo de Trabajo considere la posibilidad de utilizar otro término en lugar de “identificación electrónica”.

Además, la utilización del adjetivo “electrónica” en este término, que tiene por objeto describir el “proceso utilizado para obtener una garantía suficiente de la vinculación entre [un sujeto] […] y una identidad” podría generar confusión en cuanto a la naturaleza de los procesos, los sistemas y los servicios que se tratan en el proyecto de disposiciones. Lo mismo sucede con las definiciones de “servicios de gestión de la identidad” y “sistema de gestión de la identidad”, en las que se especifica que han de llevarse a cabo “en forma electrónica”. Al describir el proceso de vinculación como “electrónico”, o los servicios o sistemas de gestión de la identidad como “en forma electrónica” se pasa por alto el hecho de que, en algunos casos, el proceso, en su totalidad o en parte, podría no ser electrónico. Por ejemplo, algunas funciones pueden realizarse en forma no electrónica, o estar basadas en documentos en papel, como la comprobación de identidad. Por consiguiente, se recomienda que el Grupo de Trabajo considere la posibilidad de reconocer que es probable que los procesos, sistemas y servicios comprendidos en el ámbito de aplicación del proyecto de disposiciones incluyan diversos elementos no electrónicos.

d) **Identidad**: La definición de “identidad” como un conjunto de atributos que permiten a [un sujeto][una persona] “distinguirse de manera inequívoca” en un contexto particular podría considerarse excesivamente restrictiva. En muchos casos, la identificación se utiliza a efectos de cualificación, más que de distinción inequívoca. La identificación puede utilizarse simplemente para verificar si una persona pertenece a un grupo determinado, por ejemplo, “¿es usted mayor de 21 años?”, “¿es usted

miembro de un club”?, “¿tiene usted la ciudadanía?”, etc. Cabe suponer que muchas personas poseen esos atributos, por lo que la identidad no tendría por qué distinguirlas de manera inequívoca, pero sí serviría para distinguir suficientemente al sujeto de los datos en el contexto en que sea necesario limitar de ese modo la identidad.

e) **Credenciales de identidad**: El Grupo de Trabajo debería tener presentes los avances y novedades que se produzcan en relación con los medios para comunicar la información sobre la identidad. Si bien las credenciales de identidad son el medio más habitual para verificar y confirmar la identificación, cabe destacar que muchos de los nuevos sistemas de gestión de la identidad no utilizan credenciales de identidad *per se*. Así pues, la definición no es de por sí inadecuada, pero se ha de tratar de evitar incorporar en el proyecto de disposiciones la presunción de que siempre se van a utilizar credenciales de identidad. Téngase en cuenta además que la definición se limita a la “forma electrónica”. El Grupo de Trabajo tal vez debería considerar la posibilidad de ampliar el ámbito de aplicación del proyecto de disposiciones a las formas tradicionales de identificación en papel o en persona.

f) **Comprobación de identidad**: No es necesario que el proceso de comprobación de identidad defina y confirme por completo la identidad de un sujeto. Es decir, la comprobación de identidad podría consistir en recopilar, verificar o validar uno o más atributos que, si bien por sí solos no serían suficientes para definir y confirmar una identidad, podrían ser utilizados por otros para confirmar una identidad. Así pues, el Grupo de Trabajo tal vez desee considerar la posibilidad de adoptar una definición más amplia de este término.

g) **Parte que confía**: Quizá no sea apropiado eliminar esta definición y sustituirla por el término “abonado”. El concepto de “abonado” implica un participante activo en el sistema que está obligado a cumplir las normas. Si bien este puede ser una parte que confía, hay otras personas o entidades que también pueden celebrar un contrato de prestación de servicios de gestión de la identidad, por ejemplo, los sujetos. En consecuencia, si no se establece una distinción entre las partes que confían y los sujetos (u otros usuarios de un sistema de gestión de la identidad) podría haber confusión al aplicar las normas del proyecto de disposiciones. Se propone que el Grupo de Trabajo considere la posibilidad de mantener una definición de la “parte que confía” de modo que las cuestiones que se traten en las secciones posteriores se apliquen a las partes que confían o a los sujetos, según corresponda.

h) **Sujeto**: En el contexto de los servicios de gestión de la identidad, un sujeto es una persona u objeto que es identificado, o que al menos participa en el proceso de comprobación de identidad. Si se suprime la referencia a la identificación, el término sería genérico y, probablemente, no muy útil.

i) **Abonado**: Como se señaló anteriormente, el concepto de abonado como “persona que celebra un contrato de prestación de servicios de gestión de la identidad o servicios de confianza con un proveedor de servicios de gestión de la identidad” parecería ser excesivamente inclusivo, ya que podría abarcar muchos de los papeles de un sistema de identidad, además de los sujetos. Por ejemplo, la redacción del párrafo 3 de la opción C del artículo 12 presupone que los abonados son partes que confían. Sin embargo, los abonados también pueden ser sujetos o cualquier otro de los muchos papeles de un sistema de gestión de la identidad, en cuyo caso lo dispuesto en esa sección sería inadecuado.

2. Artículo 2. Ámbito de aplicación

El Grupo de Trabajo debería considerar la posibilidad de volver a examinar el ámbito de aplicación del proyecto de disposiciones en lo que respecta a la gestión de la identidad. Tal como está redactado, el ámbito de aplicación del artículo 2 se limita a dos temas: 1) la ***utilización*** de ***sistemas de gestión de la identidad***, y 2) el ***reconocimiento transfronterizo*** de ***sistemas de gestión de la identidad***.

El Grupo de Trabajo podría tal vez examinar si el ámbito de aplicación también debería incluir las ***operaciones de gestión de la identidad***, y quizá también una referencia al ***funcionamiento*** de los sistemas de gestión de la identidad o a la ***prestación*** de servicios de gestión de la identidad.

Asimismo, puesto que reconoce que no está facultado para redactar normas para los sistemas de gestión de la identidad administrados por los Estados (por ejemplo, los sistemas de gestión de la identidad nacionales), el Grupo de Trabajo debería considerar la posibilidad de modificar el artículo 2 para aclarar que "será aplicable a [...] sistemas de gestión de la identidad ***del sector privado***".

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

De conformidad con el artículo 3, párr. 2, el consentimiento de una persona en utilizar un sistema de gestión de la identidad podrá inferirse de su conducta. Sin embargo, el Grupo de Trabajo debería tomar nota del hecho de que sería erróneo extraer esa conclusión en los casos en que se ha usurpado la identidad de la persona (por ejemplo, cuando la persona que ha robado la identidad está usando credenciales falsas, o cuando está usando credenciales auténticas, pero expedidas a otra persona). En esos casos, la persona cuyo consentimiento se infiere no es el autor de la conducta descrita.

4. Artículo 4. Interpretación

El Grupo de Trabajo tal vez podría considerar la posibilidad de velar por que el proyecto de disposiciones no haga distinciones entre modelos de sistemas de gestión de la identidad mediante la inclusión del concepto de **neutralidad de los sistema de gestión de la identidad** (o neutralidad de las operaciones de identidad). Dado que hay muchas maneras diferentes de realizar operaciones de identidad en línea (por ejemplo, sistemas con un único proveedor de identidad, sistemas federados (múltiples proveedores de identidad), sistemas controlados por los usuarios/centrados en los usuarios, sistemas de concentradores (*hub systems*), sistemas de tecnología de registros distribuidos, sistemas sin credenciales, sistemas de identidad autosoberana, etc.), es importante que el proyecto de disposiciones no adopte ni exija un enfoque concreto de los procesos de identificación o autenticación, ni del sistema que los habilita. Así pues, el Grupo de Trabajo debería estudiar cómo asegurarse de que el proyecto de disposiciones no implique ni exija un modelo de sistema determinado.

5. Artículo 5. Reconocimiento jurídico de un sistema de gestión de la identidad

Podría ser necesario examinar y analizar en mayor profundidad el artículo 5 a), en el que se afirma que no se negarán efectos jurídicos a la identificación electrónica por la sola razón de que se haya hecho en forma electrónica. Damos por supuesto (pero no lo hemos verificado) que algunas leyes relativas a la utilización de credenciales de identidad exigen la presentación de un documento en papel u otro soporte físico en lugar de electrónico. Así pues, antes de dejar sin efecto esas leyes, recomendamos que se lleve a cabo un examen y análisis en mayor profundidad para determinar las repercusiones de esta disposición.

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

Idoneidad del enfoque único: El artículo 6 impone una serie de obligaciones a los proveedores de servicios de gestión de la identidad. Las obligaciones que en él se enumeran son propias del modelo de sistema de gestión de la identidad tradicional y, en consecuencia, dan por hecho que el proveedor de servicios de gestión de la identidad desempeña todas las funciones de ese sistema tradicional, o es responsable de ellas. No obstante, se están probando diversos modelos de sistema de gestión de la identidad y, por ende, los modelos están experimentando cambios. Por ese motivo, suscita preocupación que la utilización de esa lista de obligaciones se base en un modelo antiguo que quizá no se ajuste a los sistemas de gestión de la identidad más actuales o que dificulte indebidamente que se siga experimentando con distintos modelos. En muchos de los sistemas de gestión de la identidad más recientes, por ejemplo,

algunas de las funciones de los proveedores de servicios de gestión de la identidad que se enumeran en el artículo 6 podrían ser responsabilidad de diversas entidades (como proveedores de servicios de confianza, registradores, agentes de inscripción, proveedores de servicios de credenciales, gestores de confianza (*stewards*), proveedores de servicios de autenticación, concentradores, etc.). Habida cuenta de que la diversidad de modelos de sistema de gestión de la identidad es cada vez mayor, el Grupo de Trabajo debería cuestionar la idoneidad de imponer a los proveedores de servicios de gestión de la identidad un único conjunto de obligaciones.

Fuente de las obligaciones: El Grupo de Trabajo podría examinar también una importante cuestión previa, a saber, si las obligaciones de los proveedores de servicios de gestión de la identidad del sector privado (u otros papeles de los sistemas de gestión de la identidad) deberían definirse en el proyecto de disposiciones y ser aplicables a todos los sistemas de gestión de la identidad, o si cada sistema de gestión de la identidad del sector privado debería definir cuáles son esas obligaciones en su propio marco de confianza de base contractual. Si las obligaciones de cada papel se incluyen en el marco de confianza aplicable al sistema de gestión de la identidad, el operador del sistema y los participantes podrán adaptarlas al fin y al uso que se vaya a dar a cada sistema y además cumplir la ley aplicable.

Normas por las que se rige el sistema de gestión de la identidad: Por último, cabe señalar que en este artículo se mencionan las normas por las que se rige el sistema de gestión de la identidad, pero no se definen. Por ejemplo, no está claro si esas normas se refieren al marco de confianza de base contractual aplicable a un determinado sistema de gestión de la identidad o a otra cosa.

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

Responsabilidad de adoptar medidas en caso de violación de los datos: Tal como está redactado, el artículo 7 parecería no distinguir entre los sistemas de gestión de la identidad y los proveedores de servicios de gestión de la identidad, y parecería también dar por sentado que el sistema de gestión de la identidad estará controlado por un único proveedor de servicios de gestión de la identidad que realiza todas las funciones del sistema. Además, el artículo 7 impone obligaciones al proveedor de servicios de gestión de la identidad en caso de que "se produzca" una falla de seguridad, con independencia del conocimiento que tenga de esa falla o de su responsabilidad o control sobre ella. Sin embargo, en la realidad, en un sistema de gestión de la identidad pueden intervenir múltiples partes, muchas de las cuales podrían no tener ningún control o responsabilidad sobre el servidor, la red o el sistema, los empleados u otras personas o dispositivos que sean objeto de la falla.

En muchos de los enfoques más recientes de los sistemas de gestión de la identidad, algunas de estas funciones pueden ser responsabilidad de entidades diferentes (por ejemplo, proveedores de servicios de confianza, registradores, agentes de inscripción, proveedores de servicios de credenciales, proveedores de servicios de autenticación, concentradores, etc.). El origen de la falla podría estar en cualquiera de esos papeles, y cabe la posibilidad de que el proveedor de servicios de gestión de la identidad ni siquiera tenga conocimiento de ella.

Así pues, cuando se aborda la cuestión de la violación de datos, el Grupo de Trabajo debería examinar la *distinción entre los sistemas de gestión de la identidad y los proveedores de servicios de gestión de la identidad* y el hecho de que en un único sistema de gestión de la identidad pueden participar *múltiples proveedores de servicios de gestión de la identidad* (y otros muchos papeles). Por consiguiente, la primera cuestión sería determinar a quién incumbe la responsabilidad por el objeto de la falla y a quién la obligación de notificar.

Lo ideal sería que las obligaciones que impone el artículo 7 en caso de falla (por ejemplo, subsanar la falla, revocar las credenciales, notificar a las autoridades o notificar a los sujetos de datos afectados por la falla o a las partes que confían) deberían imponerse únicamente a la parte que realmente haya sufrido la falla, o que sea

responsable del servidor, la red o el sistema que haya sufrido la falla o se haya visto comprometido. Por ejemplo, en el caso de un sistema de gestión de la identidad que incluya múltiples proveedores de servicios de gestión de la identidad o múltiples papeles, podría ser conveniente adoptar las siguientes medidas: i) imponer el deber de subsanar la falla a la entidad que la haya sufrido y que esté en condiciones de contenerla y subsanarla, y ii) imponer el deber de notificar a los sujetos a la entidad que tenga la relación con ellos.

Falla a nivel de sistema: En relación con lo anterior, el Grupo de Trabajo debería también considerar la posibilidad de revisar el artículo 7 de modo que contemple la posibilidad de que una falla importante a nivel de sistema en un sistema de múltiples proveedores de servicios de gestión de la identidad (por ejemplo, si una clave privada raíz queda comprometida) comprometa el sistema en su totalidad y a todos sus proveedores de servicios de gestión de la identidad, en función del tipo y la estructura del sistema. En un caso así, una falla podría afectar a todos los proveedores de servicios de gestión de la identidad, con independencia de cuál sea su responsabilidad por la falla en sí. Por consiguiente, es probable que se necesite un tipo de respuesta diferente y que todos los proveedores de servicios de gestión de la identidad tengan que asumir determinadas obligaciones para hacer frente a la situación, aun cuando no hayan tenido ninguna responsabilidad por la falla.

Responsabilidad por la pérdida: Por último, cabe señalar que en el artículo 7, párr. 1 b), se exige al proveedor de servicios de gestión de la identidad "subsanar la falla o ***la pérdida***". Si bien podría ser necesario exigir a un proveedor de servicios de gestión de la identidad que subsane una falla (al menos una falla que esté bajo su control), el Grupo de Trabajo debería examinar la conveniencia de exigir al proveedor de servicios de gestión de la identidad que subsane también la pérdida. La pérdida puede ser considerable y, para determinar si un proveedor de servicios de gestión de la identidad es responsable de las pérdidas sufridas, y en qué medida, deberían aplicarse las normas sobre responsabilidad pertinentes, con independencia de cómo se determinen.

8. Artículo 8. Obligaciones de los abonados

Obligaciones que se han de abordar: Como observación general, si en el presente proyecto de disposiciones se van a abordar las obligaciones de los participantes en el sistema de gestión de la identidad (por ejemplo, artículos 6, 7 y 8), el Grupo de Trabajo podría quizá considerar la posibilidad de abordar las obligaciones de ***todos*** los participantes en el sistema (es decir, las obligaciones de los agentes de inscripción, los proveedores de atributos, los proveedores de servicios de gestión de la identidad, los usuarios, los concentradores, las partes que confían, los proveedores de servicios de confianza, los abonados, etc.). Esto también revestiría importancia a efectos de asignación de responsabilidades conforme al artículo 12.

Dónde se han de abordar las obligaciones: El Grupo de Trabajo tal vez podría examinar también cuál sería el lugar más adecuado para abordar las obligaciones de los proveedores de servicios de gestión de la identidad, los abonados y otros participantes en los sistemas de gestión de la identidad. En los artículos 6, 7 y 8 del proyecto de disposiciones se adopta un enfoque único para abordar las obligaciones de los proveedores y los abonados de los servicios de gestión de la identidad. No obstante, dada la diversidad de los sistemas de gestión de la identidad, podría ser más apropiado permitir o exigir que cada sistema de gestión de la identidad aborde las obligaciones de todos los diferentes papeles en un marco de confianza adaptado específicamente a su tecnología, metodología y finalidad, en lugar de utilizar el proyecto de disposiciones para imponer un enfoque único a todos los sistemas de gestión de la identidad. Esto se debe, en parte, a que es muy probable que las categorías y definiciones de los papeles de los sistemas de gestión de la identidad, así como las obligaciones de los participantes que los desempeñan, varíen enormemente de unos sistemas a otros. Uno de los factores que da lugar a esas variaciones es el objetivo para el que se establece un sistema de gestión de la identidad concreto (por ejemplo, para facilitar las comunicaciones en línea en el sector farmacéutico, como el sistema SAFE BioPharma, para facilitar el intercambio de información académica, como el sistema InCommon utilizado por las

universidades, o para facilitar las comunicaciones con los organismos públicos, como el sistema eIDAS).

Además, como se señaló anteriormente en relación con el artículo 6, se están probando diversos modelos de sistema de gestión de la identidad y, por ende, estos están experimentando cambios, lo que lleva a cuestionar la conveniencia de incluir una lista predefinida de obligaciones en vista del riesgo que podría entrañar que esta imponga un modelo desactualizado que no se ajuste bien a muchos de los actuales sistemas de gestión de la identidad y dificulte indebidamente la experimentación con distintos modelos.

Obligaciones de los abonados: El artículo 8 trata sobre los abonados (es decir, las personas que celebran un contrato de prestación de servicios de gestión de la identidad). Esto incluiría, supuestamente, a muchos de los participantes en un sistema de gestión de la identidad, como las partes que confían, los sujetos de datos individuales y, posiblemente, otros papeles del sistema. El artículo 8 impone a los abonados la obligación de notificar al proveedor de servicios de gestión de la identidad cuando tengan conocimiento de que las credenciales de identidad o los mecanismos de identificación electrónica del sistema de gestión de la identidad han quedado comprometidos, o cuando tengan conocimiento de circunstancias que dan lugar a un riesgo considerable de que queden comprometidos.

En lo que respecta a las personas físicas (por ejemplo, sujetos de datos), eso podría constituir un requisito oneroso y poco razonable. Por ejemplo, cabe suponer que existen numerosas situaciones en las que una persona abonada a un sistema de gestión de la identidad podría ser consciente de circunstancias que comportan un riesgo, pero no ser consciente de su importancia. Además, dado que esta obligación parecería aplicarse a la totalidad del sistema de gestión de la identidad (en lugar de, por ejemplo, a las credenciales de identidad expedidas a una persona concreta), esta disposición parecería imponer una carga considerable a las personas físicas (y, en realidad, a otros abonados del sistema), que podrían ser conocedoras de determinada información, pero no comprender su importancia para todo el sistema.

Aun cuando las credenciales de identidad de una persona física se hayan perdido o hayan quedado comprometidas, no siempre procede imponer a la persona la obligación de comunicar la pérdida. Al igual que sucede con los números de las tarjetas de crédito robadas, exigir al sujeto que notifique esos incidentes podría simplemente ser poco realista, o incluso inapropiado (especialmente en el caso de usuarios poco experimentados o de fallas que ocurren en Internet o en otros medios que no conocen bien). En el caso de los sistemas de gestión de la identidad que no se basan en la utilización de credenciales físicas, el sujeto podría simplemente no saber que los datos de sus credenciales (por ejemplo, el número de identidad) se han visto comprometidos.

9. Artículo 9. Identificación de [un sujeto][una persona] que utiliza un sistema de gestión de la identidad

Conveniencia de dejar sin efecto la legislación vigente: El texto del artículo 9 está retomado en gran medida de la Ley Modelo sobre las Firmas Electrónicas y la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales y parecería dejar sin efecto las leyes vigentes que definen requisitos de identificación aplicables únicamente en casos concretos. En lo que respecta a las leyes sobre firmas electrónicas, este criterio general de dejar sin efecto otras leyes sobre firmas dio buenos resultados. No obstante, el Grupo de Trabajo tal vez desee evaluar si eso mismo puede hacerse extensible a la identificación de un sujeto. Concretamente, dado que algunas leyes exigen una identificación simple, pero otras son muy específicas en lo que respecta al modo y el método de identificación (como las leyes en materia de privacidad, las leyes relativas al principio “conozca a su cliente”, las leyes relativas al notariado, etc.), una norma general que considere que se han satisfecho los requisitos de identificación simplemente porque se haya cumplido una norma de fiabilidad podría no ser apropiada.

Cabe suponer que es poco probable que un proceso general de identificación, aun cuando sea “fiable”, pueda satisfacer los diversos requisitos de identificación previstos en todas las leyes en vigor. También es posible que, cuando las partes en una operación comercial han fijado sus propios requisitos de identificación, un sustituto electrónico que cumpla la norma general de “fiabilidad” no baste para satisfacer esos requisitos específicos o inequívocos de las partes.

Posible conflicto entre artículos: El Grupo de Trabajo también debería analizar lo que parecería ser un conflicto entre el artículo 2, párrafo 3, y el artículo 9. El artículo 2, párrafo 3, reconoce que muchas de las leyes en vigor imponen a las partes del sector privado diversos requisitos de identificación y, con ese fin, afirma que “[n]ada de lo dispuesto en el presente [instrumento] afectará a obligación legal alguna de identificar a [un sujeto][una persona] de conformidad con un procedimiento determinado que la ley establezca o exija”. No obstante, el enfoque único del artículo 9 parecería contradecir esta disposición.

La opción A del artículo 9 reza como sigue:

> “Cuando una norma jurídica requiera o permita que se identifique a [un sujeto] [una persona], esa norma se dará por cumplida respecto de un sistema de gestión de la identidad si se utiliza un método fiable para la identificación electrónica [del sujeto] [de la persona].”

La opción B del artículo 9 reza como sigue:

> “Un sujeto puede ser identificado mediante el uso de servicios de gestión de la identidad si se utiliza un método fiable para la identificación electrónica [del sujeto] [de la persona].”

Habida cuenta de la diversidad de requisitos relativos a los procesos de identificación previstos en las diferentes leyes, el enfoque único del artículo 9 no parecería ser viable en la práctica. Parte del problema parecería residir en el hecho de que la identificación se trata de la misma forma que las firmas electrónicas. En el caso de las firmas electrónicas, la creación de una firma electrónica de la forma prevista en la Ley Modelo satisfará los requisitos de cualquier ley que exija una firma, pero no sucede lo mismo con los requisitos de identificación.

Los requisitos que se han de satisfacer para identificar a alguien varían enormemente en función de la ley aplicable, la finalidad con que se exige la identificación (primaria frente a funcional) y la importancia del asunto de que se trate. Por ejemplo, el recientemente publicado Reglamento de la Ley de Privacidad de los Consumidores de California establece unos requisitos de identificación exhaustivos que se deben cumplir antes de publicar o eliminar datos personales a instancias de una persona que afirme ser el sujeto[4]. Asimismo, las normas “conozca a su cliente” del sector financiero imponen requisitos de identificación específicos de diversa índole. Así pues, el Grupo de Trabajo quizás debería estudiar también si sería conveniente utilizar una declaración general única en la que se indique que la utilización de un sistema fiable satisface los requisitos legales de identificación, o en qué circunstancias sería apropiado hacerlo.

El conflicto entre estas disposiciones ilustra el problema que se plantea al tratar de formular un conjunto de normas sobre identidad utilizando los mismos criterios utilizados previamente para las firmas electrónicas.

La fiabilidad como concepto relativo: Además, es importante examinar si el artículo 9 reconoce debidamente que la fiabilidad, al igual que la seguridad, es un concepto relativo. Un método fiable en un contexto podría no serlo en otro. Por ejemplo, la utilización de Facebook o Google para efectuar la identificación electrónica de una persona suele ser suficientemente fiable a efectos de acceso a una cuenta normal en un sitio web, pero probablemente no lo sea para acceder a una cuenta bancaria y autorizar una transferencia de fondos desde esa cuenta. Así pues, si se desea supeditar la obtención

[4] Véase Reglamento de la Ley de Privacidad de los Consumidores de California, artículo 4. Puede consultarse en www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?

de un efecto jurídico al requisito de fiabilidad, se alienta al Grupo de Trabajo a considerar la posibilidad de modificar el texto del artículo 9 a fin de reconocer que el "método fiable" es un concepto relativo. Un posible enfoque consistiría en incorporar algo similar al concepto "tan fiable como sea apropiado" que se utilizó en la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, es decir, que el método empleado es: i) tan fiable como sea apropiado para los fines para los que se exigió la identificación electrónica, atendidas todas las circunstancias del caso, inclusive todo acuerdo aplicable; o ii) se ha demostrado en la práctica que es suficientemente fiable.

Procesos múltiples pertinentes a la fiabilidad: Al aplicar el requisito de fiabilidad únicamente al método empleado con fines de identificación electrónica[5], el artículo 9 parecería también ignorar el resto de los procesos que se requieren para la identificación, que también podrían incidir en la fiabilidad de los resultados, y los métodos que podrían emplearse en esos procesos. Entre esos procesos figuran los de comprobación de identidad, los procesos de inscripción, las credenciales de seguridad, los procesos de autenticación, los procesos de identificación electrónica, el *software*, la seguridad de los datos, los empleados, etc. Por ejemplo, aun cuando se emplee un método objetivamente fiable para la identificación electrónica de una persona, no tendrá ningún valor si el proceso de comprobación de identidad no fue también suficientemente fiable.

10. Artículo 10. Factores pertinentes para la determinación de la fiabilidad

El artículo 10 especifica únicamente los factores pertinentes para determinar la fiabilidad de un "método [...] para la identificación electrónica"[6] al que se alude en el artículo 9. Sin embargo, no especifica qué factores deberían evaluarse para determinar la fiabilidad de otros procesos clave realizados por un sistema de gestión de la identidad, como la comprobación de identidad.

El artículo 10 se centra en las siguientes cuatro categorías de factores:

- cumplimiento de las obligaciones establecidas en el artículo 6
- 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
- toda supervisión o certificación que se hubiera realizado con respecto al sistema de gestión de la identidad
- todo "pacto que hubieran acordado las partes".

No obstante, si bien los cuatro factores anteriormente enumerados se centran en el cumplimiento de las reglas o normas, la certificación y el pacto entre las partes, no necesariamente establecen la fiabilidad. El hecho de que las reglas y normas, la certificación o los pactos existen y se cumplen no significa necesariamente que un sistema de gestión de la identidad que los cumpla sea fiable para cualquier fin. Así pues, si el Grupo de Trabajo decide abordar los factores para determinar la fiabilidad de un "método [...] para la identificación electrónica", quizás debería examinar, en primer lugar, qué procesos son pertinentes para determinar la fiabilidad (por ejemplo, procesos de comprobación de identidad, procesos de inscripción, seguridad de las credenciales, procesos de autenticación, procesos de identificación electrónica, *software*, seguridad de los datos, empleados, etc.) y posteriormente determinar qué reglas o normas establecen la fiabilidad con respecto a cada uno de esos procesos.

[5] Véase el artículo 1 d) del proyecto de disposiciones, donde se define la identificación electrónica como "el proceso utilizado para obtener una garantía suficiente de la vinculación entre [un sujeto][una persona] y una identidad".

[6] Como se establece en el artículo 1 d), la definición de "identificación electrónica" se limita al proceso utilizado para obtener una garantía suficiente de la vinculación entre [un sujeto][una persona] y una identidad, no abarca los muchos otros procesos que se requieren en un sistema de gestión de la identidad.

Más aún, como se deduce de la lista anterior, los sistemas de gestión de la identidad utilizan muchos procesos diferentes que se pueden llevar a cabo utilizando uno o más tipos de "métodos" que pueden o no ser fiables. Asimismo, establecer que un "método [...] para la identificación electrónica" se está empleando de manera fiable, por ejemplo, no implica necesariamente que el proceso de comprobación de identidad en que se basa se haya realizado empleando un método fiable.

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

Criterios y competencia: En el artículo 11 se otorga a la persona o entidad del sector público o privado que haya especificado el Estado (la "**entidad que determina la fiabilidad**") la facultad de decidir qué sistemas de gestión de la identidad son fiables. No obstante, el artículo 11 no especifica criterio alguno en relación con la competencia de la entidad que determina la fiabilidad para tomar esa decisión. Tampoco se especifica qué proceso se debe seguir, aparte del requisito de tener en cuenta todas las circunstancias pertinentes, incluidos los factores enumerados en el artículo 10, y un requisito general de ser coherente con "las normas y procedimientos internacionales reconocidos y pertinentes para determinar la fiabilidad", que no se especifican. En consecuencia, suscita preocupación la posibilidad de que unas entidades no cualificadas evalúen la fiabilidad empleando criterios inadecuados y, por ende, se designen como fiables sistemas de gestión de la identidad que no lo son. Además, las designaciones de sistemas de gestión de la identidad fiables pueden variar considerablemente de un Estado a otro, incluso para un mismo sistema. Habida cuenta de la importancia de esas designaciones conforme al artículo 9 (es decir, el artículo 9 presupone que los sistemas designados utilizan "métodos fiables", con los consiguientes efectos jurídicos), esto podría entrañar problemas importantes.

El Grupo de Trabajo tal vez debería estudiar también qué criterios podrían utilizar los Estados para determinar si la entidad que determina la fiabilidad es competente y cómo se asegurarían de que esa entidad cuente con los conocimientos especializados, los procesos y los recursos necesarios para decidir qué sistemas de gestión de la identidad son "fiables". Por ejemplo, ¿debería la entidad designada por el Estado someterse a un proceso de certificación antes de que se le confiera esa facultad?

Fiabilidad de los sistemas frente a fiabilidad de las operaciones: Puesto que la fiabilidad es un concepto relativo, cabe suponer que las evaluaciones de la fiabilidad deberán preguntarse "¿fiable para qué fin?". Esto platea la cuestión previa de si el Grupo de Trabajo debería centrarse en la fiabilidad de los sistemas de gestión de la identidad en general (independientemente del tipo de operación de identidad para la que se utilicen) o la fiabilidad de las operaciones de gestión de la identidad (que proporcionan un contexto específico en que evaluar la fiabilidad).

Fiabilidad de los sistemas de gestión de la identidad frente a fiabilidad de un "método [...] para la identificación electrónica": El artículo 11 se centra en la fiabilidad de los "sistemas de gestión de la identidad", mientras que el artículo 9 determina el efecto jurídico de una identificación basada en la fiabilidad del "método [...] para la identificación electrónica". Ambos enfoques parecerían ser incoherentes, en particular porque la fiabilidad de un método de identificación electrónica no es sino un subconjunto de la fiabilidad general de las funciones de un sistema de gestión de la identidad.

Cuestiones prácticas: El acento que el artículo 11 pone en la entidad que determina la fiabilidad (y su importancia para obtener el efecto jurídico previsto en el artículo 9) parece indicar que es necesario que los sistemas de gestión de la identidad sean evaluados en cada Estado por un mecanismo institucional centralizado y que las autoridades públicas se impliquen, al menos para designar a dicha entidad. Alentamos al Grupo de Trabajo a que analice si esto es práctico.

Además, el Grupo de Trabajo tal vez desee examinar si la necesidad de obtener las ventajas que aporta ser un sistema de gestión de la identidad fiable designado discriminará a aquellos sistemas de gestión de la identidad que no puedan permitirse los

gastos que conlleva el proceso de designación de la fiabilidad. El Grupo de Trabajo podría examinar también las siguientes cuestiones:

- ¿A qué entidades procedería facultar para determinar la fiabilidad?
- ¿Cómo se puede determinar si una entidad está cualificada y es competente?
- ¿En qué medida es fiable la decisión de una entidad que determina la fiabilidad (dado que se trata de una evaluación que se realiza en un momento concreto)? ¿Con qué frecuencia se tiene que repetir?
- ¿Competería al Estado nombrar entidades que determinan la fiabilidad para los sistemas de gestión de la identidad del sector privado, o supeditar determinados efectos jurídicos a la obtención de esa designación de fiabilidad?
- ¿Tendría esto el efecto en la práctica de exigir a todos los sistemas de gestión de la identidad que cumplan las normas fijadas por el Estado o la entidad que determina la fiabilidad (dado que todos querrán ser designados fiables) y, por consiguiente, impedir futuros avances?
- ¿Qué se considera una "norma internacional reconocida"? ¿Quién la reconoce como tal? ¿Qué ocurre si la norma cambia?
- ¿Cabe la posibilidad de que la imposición de una norma determinada y el cumplimiento de esta exijan procedimientos de certificación que podrían llegar a ser costosos y complejos?
- ¿Qué relación guardan los factores para determinar qué métodos son fiables (artículo 10) con los requisitos para determinar qué sistemas de gestión de la identidad son fiables (artículo 11)?

Por último, dado que en el artículo 11 se contempla la posibilidad de designar sistemas de gestión de la identidad con independencia de su ubicación geográfica, el Grupo de Trabajo debería estudiar si esto se traducirá en que, en la práctica, los sistemas de gestión de la identidad se verán obligados a obtener esa designación en cada uno de los Estados en que sus abonados realizan sus actividades comerciales, y si esto será un obstáculo para las operaciones transfronterizas.

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

El Grupo de Trabajo tal vez desee estudiar algunos aspectos de las disposiciones sobre responsabilidad del proyecto que suscitan preocupación.

Premisa: El artículo 12 (al menos las opciones B y C), al igual que el artículo 6, parecerían partir de la premisa de que se pueden aplicar las mismas normas a todos los sistemas de identidad. No obstante, habida cuenta de que el tipo, la finalidad, el alcance, las funcionalidades, el funcionamiento y los papeles y responsabilidades de los participantes de los sistemas de gestión de la identidad son cada vez más diversos, parecería altamente improbable que las normas que se especifican en el artículo 6, o las normas de fiabilidad que se especifican en las opciones B o C del artículo 12, sean apropiadas en todos los casos. Basta con comparar las diferencias entre los sistemas de identidad basados en infraestructura de clave pública, los sistemas basados en tecnologías de cadenas de bloques, los centrados en el usuario y los sistemas de identidad autosoberana para darse cuenta de que será imposible que esas normas encajen en todos los casos. Dado que puede haber grandes diferencias entre los sistemas de gestión de la identidad, la misma distribución de responsabilidades podría no ser apropiada para todos los sistemas. Así pues, el Grupo de Trabajo tal vez desee plantearse la conveniencia de adoptar un enfoque único de la responsabilidad.

Papeles comprendidos: El artículo 12 únicamente trata sobre la responsabilidad de los proveedores de servicios de gestión de la identidad. Si el Grupo de Trabajo considera que la cuestión de la responsabilidad se debe abordar en el proyecto de disposiciones, tal vez sería apropiado estudiar la cuestión de la distribución de responsabilidades entre todos los participantes. Esto incluiría, por ejemplo, la responsabilidad de los

proveedores de servicios de gestión de la identidad, los agentes de inscripción, los proveedores de atributos, los proveedores de identidad, los sujetos, los usuarios, los *hubs*, los proveedores de servicios de verificación, los proveedores de servicios de confianza, las partes que confían, etc. Esto es importante porque abordar la responsabilidad de un solo papel ni mitiga ni elimina los daños y perjuicios que pudieran derivarse de un problema, sino que simplemente traspasa esa pérdida a otro. Para distribuir adecuadamente las responsabilidades sería preciso tener presente a quién correspondería soportar la pérdida.

Derecho a que se limite o excluya la responsabilidad: El Grupo de Trabajo tal vez desee examinar si los proveedores de servicios de gestión de la identidad (u otros participantes en el sistema) deberían tener derecho a limitar o excluir su responsabilidad, por vía contractual o por otras vías. La opción A podría permitir limitaciones o exenciones, al menos en la medida en que lo permita la ley aplicable. Cabe suponer que esto implica un reconocimiento del hecho de que existen otros muchos supuestos y tipos de responsabilidad que los proveedores de servicios de gestión de la identidad u otros pueden tratar legítimamente de limitar o excluir, y al menos reconoce la flexibilidad de las opciones de limitación y exclusión de la responsabilidad disponibles conforme a la ley aplicable.

Si bien la opción C prevé un derecho limitado a eximirse de responsabilidad, su ámbito es muy reducido y no deja ningún margen de flexibilidad. Se plantea asimismo la cuestión de si las disposiciones de las opciones B o C, en general, impiden que los proveedores de servicios de identidad se eximan totalmente de responsabilidad (como suelen hacer los organismos públicos).

Además, en vista de que las opciones B y C limitan la responsabilidad de los proveedores de servicios de gestión de la identidad al incumplimiento de las obligaciones que les incumben en virtud del artículo 6, cabría preguntarse qué ocurriría en caso de robo de identidad. Es decir, si un proveedor de servicios de gestión de la identidad emite unas credenciales a alguien que ha robado una identidad, o lo identifica electrónicamente, sin incumplir lo dispuesto en el artículo 6, ¿quién soportaría la pérdida? ¿Debería hacerlo la víctima de un robo de identidad que podría no haber tenido comunicación alguna ni haber entablado una relación contractual con el proveedor de servicios de gestión de la identidad?

Limitación de la responsabilidad según la opción C: El párrafo 3 de la opción C del artículo 12 se basa en los siguientes supuestos: 1) se pueden imponer limitaciones en cuanto a los fines o el valor de determinadas operaciones de identidad (si bien no se especifica dónde o cómo se imponen esas limitaciones), y 2) la parte que confía ha podido tener conocimiento fácilmente de esas limitaciones antes de depositar su confianza. Esto parecería ser un vestigio de los criterios empleados inicialmente en algunos de los primeros sistemas de infraestructura de clave pública, en los que el certificado emitido por la autoridad certificadora solía contener una limitación en cuanto a los fines o el valor en dólares que la parte que confía debía examinar antes de depositar su confianza. Habida cuenta de la amplia variedad de sistemas de gestión de la identidad que existen hoy en día, el Grupo de Trabajo tal vez desee examinar si es viable imponer una limitación de la responsabilidad basada en las operaciones. Por ejemplo, el artículo 12 podría modificarse para reconocer que esas limitaciones podrían especificarse en el marco de confianza o en el contrato del proveedor de servicios de gestión de la identidad, en lugar de en operaciones individuales.

Interfaz con los sistemas del sector público: Por último, el Grupo de Trabajo tal vez desee examinar la posible interacción con sistemas de gestión de la identidad del sector público. En muchos casos, los proveedores de servicios de gestión de la identidad se valen de las afirmaciones sobre atributos realizadas por terceros, como sistemas de gestión de la identidad nacionales y otras bases de datos estatales (por ejemplo, el Departamento de Vehículos Motorizados (DMV)). Dado que los sistemas de gestión de la identidad del sector público a menudo se consideran dignos de confianza, pese a que tampoco suelen asumir responsabilidad alguna por los errores que se pudieran producir, debería considerarse la posibilidad de determinar quién soporta la pérdida en

caso de que la información proporcionada por el Estado sea errónea. Así pues, siempre que intervengan entidades públicas podría ser necesario adoptar un enfoque diferente.

Instamos al Grupo de Trabajo a que considere la posibilidad de no tratar de asignar responsabilidades, sobre todo en vista de la amplia variedad de sistemas de gestión de la identidad, procesos y participantes. Si el Grupo de Trabajo decide abordar la cuestión de la responsabilidad, lo alentamos a que se ocupe únicamente de los métodos que se pueden emplear para determinar la responsabilidad, pero no de las reglas, especificaciones o normas sobre responsabilidad en sí. Entre esos métodos cabe mencionar, por ejemplo, la referencia a la ley aplicable (como en la opción A), o al marco de confianza de base contractual adoptado por un sistema de gestión de la identidad y convenido por las partes en un contrato.

13. Artículo 26. Reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza

- En lo que respecta a la cuestión del "reconocimiento" transfronterizo, el Grupo de Trabajo podría tal vez aclarar las respuestas a tres preguntas fundamentales: ¿Reconocimiento de qué? ¿Reconocimiento de quién? ¿Reconocimiento con qué fin?

- ¿Reconocimiento de qué? El artículo 26, párrafo 1, parecería responder a esta pregunta centrándose en los "sistemas de gestión de la identidad" y los "efectos jurídicos" de los "sistemas de gestión de la identidad". No obstante, no está claro de qué modo pueden producir efectos jurídicos los sistemas de gestión de la identidad, ni cuáles serían esos efectos. Cabe suponer que la confianza en los procesos de comprobación de identidad o de identificación electrónica realizados por un sistema de gestión de la identidad podría tener un efecto jurídico, pero no está claro hasta qué punto puede considerarse que un sistema de gestión de la identidad en sí puede producir efectos jurídicos.

Por analogía, los Estados reconocen los pasaportes expedidos por otros Estados conforme a las normas de la OACI. Es de suponer que cada Estado acepta la validez de las normas de la OACI y puede o no evaluar si el sistema de expedición de pasaportes de otro Estado cumple esas normas, pero a lo que confiere "efecto jurídico" en la frontera es a las credenciales, es decir, al pasaporte expedido por el sistema de cada Estado.

- ¿Reconocimiento por parte de quién? Cabe suponer que la entidad que reconoce un sistema de gestión de la identidad extranjero es: 1) una entidad pública, como una administración pública o un tribunal que aplica la ley o el ordenamiento jurídico que proceda (por ejemplo, para satisfacer un requisito de verificar la identidad o determinar si una prueba es admisible), o 2) una parte que confía (sector público o privado). El artículo 26 del proyecto parecería centrarse en la primera opción, ya que hace referencia a los "efectos jurídicos" de lo que sea que se esté reconociendo. Además, la segunda opción no requiere una ley ni una conclusión jurídica, ya que las partes que confían son sin duda libres de tomar sus propias decisiones sobre si reconocerán o confiarán en un sistema de gestión de la identidad o en una identidad a los efectos de la operación que estén realizando.

- ¿Reconocimiento con qué fin? ¿Qué significa que un "sistema de gestión de la identidad" sea reconocido por la ley de un Estado extranjero? El concepto de sistema de gestión de la identidad que tiene efectos jurídicos es en cierto modo confuso. Por ejemplo, ¿significa eso que el Estado extranjero aceptará automáticamente los resultados de una identificación electrónica efectuada por el sistema de gestión de la identidad reconocido, o significa simplemente que el sistema de gestión de la identidad reconocido podrá realizar operaciones comerciales en la jurisdicción extranjera, pero podría ser necesario que modifique sus procesos para satisfacer los requisitos que imponga la jurisdicción extrajera a sus propios sistemas de gestión de la identidad?

El Grupo de Trabajo debería considerar la posibilidad de aclarar qué significa la afirmación de que cuando el funcionamiento de un sistema de gestión de la identidad tenga lugar fuera [del Estado promulgante], dicho sistema o dicho servicio producirán en [el Estado promulgante] los mismos efectos jurídicos.

14. Artículo 27. Cooperación

No está claro cuál es el propósito del artículo 27. Este parecería centrarse en el intercambio de información, experiencia y buenas prácticas, a lo que no se puede oponer objeción alguna y, en condiciones ideales, se ha de alentar, específicamente si el intercambio es voluntario y no implica la negociación de acuerdos que sean vinculantes para las entidades que no sean parte en la cooperación. No obstante, en ese caso no parecería ser necesario exigir que el Estado promulgante atribuya expresamente competencia a la entidad que intercambia información. Tampoco sería necesario centrar la cooperación en las tres categorías que se especifican en el artículo 27.

Si la cooperación y el intercambio son obligatorios, o sirven de base para el reconocimiento jurídico por un Estado o la negociación de acuerdos vinculantes para las entidades que no son parte en la negociación, esto suscitaría varias preocupaciones que el Grupo de Trabajo debería analizar en mayor profundidad y clarificar.

Obsérvese además que el artículo 27 permite (o exige) que la entidad u organismo a que el Estado promulgante haya atribuido expresamente competencia coopere con “entidades extranjeras”. No está claro a qué se refiere el término “entidades extranjeras” (por ejemplo, ¿se trata de un Gobierno extranjero, o de un proveedor de servicios de gestión de la identidad que opere en el Estado extranjero?). Cabe suponer que esa cooperación con “entidades extranjeras” debería limitarse a las entidades extranjeras a las que el Estado extranjero haya atribuido competencia.