Naciones Unidas A/CN.9/WG.IV/WP.145

Asamblea General

Distr. limitada
20 de febrero de 2017
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
55º período de sesiones
Nueva York, 24 a 28 de abril de 2017

Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza

Propuesta de los Estados Unidos de América

Nota de la Secretaría

Los Estados Unidos de América presentaron a la Secretaría un documento para que el Grupo de Trabajo lo examinara en su 55º período de sesiones. Dicho documento se reproduce como anexo a la presente nota en la forma en que lo recibió la Secretaría.

V.17-01092 (S) 020317 020317

Anexo

I. Introducción

En su 54º período de sesiones, el Grupo de Trabajo IV (Comercio Electrónico) comenzó sus deliberaciones sobre el tema de la gestión de la identidad y los servicios de confianza. Las primeras conclusiones provisionales del Grupo de Trabajo fueron las siguientes:

> 118. Tras deliberar, el Grupo de Trabajo convino en que su labor futura sobre la gestión de la identidad y los servicios de confianza se limitara a los sistemas de gestión de la identidad utilizados con fines comerciales y no tuviera en cuenta el carácter público o privado del proveedor de servicios de gestión de la identidad.
>
> 119. El Grupo de Trabajo también convino en otorgar prioridad a la labor sobre la gestión de la identidad. Además, acordó que se prestara especial atención a los sistemas de identidad pluripartitos y a las personas físicas y jurídicas, sin excluir, cuando procediera, el examen de los sistemas de identidad bipartitos y de los objetos físicos y digitales.
>
> 120. Asimismo, el Grupo de Trabajo decidió proseguir su labor aclarando en mayor medida los objetivos de la tarea propuesta, especificando su alcance, determinando los principios generales aplicables y redactando las definiciones necesarias.

(A/CN.9/897, párrs. 118 a 120).

Con objeto de contribuir a centrar las deliberaciones del Grupo de Trabajo en su 55º período de sesiones y posteriormente, la delegación de los Estados Unidos de América ha preparado el presente documento a fin de intentar presentar un panorama general de cuestiones para que las examine el Grupo de Trabajo. Aunque no cabe duda de que existen muchas más cuestiones que tendrá que examinar el Grupo de Trabajo, es de esperar que la siguiente lista inicial pueda servir como punto de partida para orientar las primeras deliberaciones y ayudar a concentrar las labores del Grupo de Trabajo. Abrigamos la esperanza de que el examen de estas cuestiones, así como de otras que pueda determinar el Grupo de Trabajo, pueda orientar a la Secretaría para la preparación de un documento de trabajo sobre la gestión de la identidad.

Entendemos que, en el plazo transcurrido entre períodos de sesiones, los expertos han entablado un debate oficioso sobre la terminología pertinente. Si bien creemos que en última instancia será necesario examinar minuciosamente la formulación de las definiciones de la terminología que habrá de utilizarse en este proyecto, en esta primera fase recomendamos que el Grupo de Trabajo estudie la posibilidad de utilizar las definiciones iniciales simplemente como base para facilitar su examen. Reconocemos, no obstante, que es posible que, en última instancia, resulte necesario un acuerdo sobre las definiciones jurídicas y técnicas más detalladas.

II. Metas y objetivos del proyecto

Como punto de partida, el Grupo de Trabajo tal vez desee examinar las metas y objetivos generales del proyecto. Habida cuenta de la decisión inicial de centrarse en la utilización de sistemas de gestión de la identidad con fines comerciales, el Grupo de Trabajo tal vez desee examinar cuáles de las metas y objetivos siguientes podrían resultar adecuados para este proyecto:

- Promover el desarrollo de un ecosistema de identidad del sector privado;
- Determinar y eliminar los obstáculos jurídicos a las transacciones de identidad con fines comerciales;
- Eliminar las ambigüedades relativas a la aplicabilidad del derecho vigente a las transacciones de identidad con fines comerciales;

- Alentar la utilización comercial y la confianza en las credenciales de la identidad digital de terceros;
- Facilitar la confianza necesaria para las transacciones de identidad con fines comerciales en línea;
- Prestar asistencia a las partes privadas proporcionando para ello una base para decidir si se confía o no en la información de identidad digital en operaciones comerciales;
- Determinar y eliminar los obstáculos transfronterizos a la autenticación electrónica;
- Facilitar el reconocimiento transfronterizo de la información de identidad digital;
- Fomentar la confianza en el comercio electrónico.

III. Naturaleza del producto propuesto de la labor del Grupo de Trabajo IV

Tal vez sea útil comenzar a examinar el tipo de producto que desearía desarrollar el Grupo de Trabajo en la esfera de la gestión de la identidad con fines comerciales.

IV. Principios rectores

Sea cual fuere la forma que adopte en última instancia el producto de la labor que ha de realizar el Grupo de Trabajo, existen varios principios generales que el Grupo de Trabajo tal vez desee tener en cuenta y, si procede, adoptar, para orientar su labor en relación con la gestión de la identidad. Al igual que la Ley Modelo sobre Comercio Electrónico y la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, esos principios generales pueden servir para guiar al Grupo de Trabajo en sus deliberaciones. Además, los principios rectores pueden resultar útiles para ayudar a aclarar el alcance de la labor. Entre los posibles principios rectores que el Grupo de Trabajo tal vez desee tener en cuenta figuran los siguientes:

A. Fuente de la obligación jurídica de identificar

Como punto de partida, el Grupo de Trabajo tal vez desee examinar si la posible legislación sobre la gestión de la identidad debería contener obligaciones de identificar a una parte en una operación comercial distintas de las que se apliquen como consecuencia de otros instrumentos legislativos. Si la legislación en materia de gestión de la identidad no contiene ninguna obligación de identificar a una parte, los requisitos legales de identificar a una parte en una operación comercial se dejarían para otras leyes vigentes como las que rigen la certificación por notario, los requisitos relativos a la obligación de conocer al cliente, las leyes contra el blanqueo de dinero o las que rigen el acceso a datos personales. Ese fue el enfoque que el Grupo de Trabajo adoptó con respecto a las firmas electrónicas cuando elaboró la Ley Modelo sobre Comercio Electrónico y la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales.

B. Autonomía de las partes

Dado que los sistemas de gestión de la identidad se regirán habitualmente por las normas de los sistemas de base contractual convenidos por los participantes en esos sistemas, tal vez sea importante tener en cuenta si todo posible instrumento legislativo

que rija las operaciones de gestión de la identidad debería reconocer esas normas de los sistemas y deferirse a ellas, y en qué medida.

Así pues, el Grupo de Trabajo tal vez desee examinar si el principio de la autonomía de las partes debería aplicarse a los sistemas comerciales de gestión de la identidad para permitir que las partes en un sistema de identidad modifiquen de mutuo acuerdo las disposiciones de cualquier norma jurídica o de determinadas normas jurídicas.

C. Neutralidad de la tecnología

Es posible que se desarrollen e implanten muchos tipos diferentes de sistemas de gestión de la identidad para su utilización en operaciones comerciales. En esos sistemas se podrá utilizar una amplia variedad de tecnologías, que pueden incluir nombres de usuario y contraseñas, sistemas más complejos basados en la norma x.509 de infraestructura de clave pública u otras normas, como SAML u OpenID Connect. Además, en la actualidad se están desarrollando sistemas en los que se utilizan otras tecnologías, como Blockchain.

Por tanto, el Grupo de Trabajo tal vez desee estudiar si los posibles productos relacionados con la gestión de la identidad deberían dejar claro que las normas de gestión de la identidad no deberían exigir la utilización de ninguna tecnología en particular.

El Grupo de Trabajo tal vez desee examinar asimismo la forma en que la CNUDMI podría ocuparse mejor de la existencia y la utilización de varios sistemas comerciales de identidad.

Por supuesto, la legislación distinta de la específica de la gestión de la identidad podrá exigir que las partes utilicen sistemas de identidad que cumplan determinados requisitos. Y las propias partes podrán insistir en que las personas y entidades con las que hacen negocios utilicen un sistema de identidad concreto. Por ejemplo, una entidad comercial podría restringir el acceso a sus servicios a aquellos usuarios que utilicen uno o más sistemas de identidad específicos de los que la entidad sea miembro.

D. Neutralidad del modelo del sistema

Además de las variaciones entre las tecnologías utilizadas, los sistemas de identidad comerciales son objeto actualmente de un alto grado de experimentación con respecto a las estructuras y enfoques institucionales y empresariales utilizados. Probablemente cabe prever una variación bastante amplia entre los modelos de sistemas de identidad en el futuro, aunque utilicen la misma tecnología básica. Incluyen los sistemas de intermediarios o de centro distribuidor, los modelos de proveedor único de identidad, los modelos de parte que confía única, los modelos institucionales y muchos más enfoques diferentes.

En consecuencia, el Grupo de Trabajo tal vez desee examinar si debería adoptar como principio el concepto de neutralidad del modelo del sistema, es decir, el reconocimiento de que cualquier producto desarrollado no debería redactarse de manera que dé por supuesto o exija la utilización de un modelo de sistema de identidad empresarial, institucional o estructural, y que pueda dar cabida con facilidad a las modificaciones futuras del enfoque, la estructura y el modelo empresarial del sistema de identidad.

E. No discriminación

El Grupo de Trabajo tal vez desee también estudiar la aplicabilidad del principio de no discriminación en el contexto de la utilización de sistemas de identidad con fines comerciales. Con arreglo a ese principio, por ejemplo, el efecto jurídico (o sea, el

cumplimiento de un requisito legal de identificación) y la admisibilidad como prueba en procedimientos judiciales de una identificación electrónica no deberían denegarse exclusivamente por razón de que esa identificación se efectuó de forma electrónica.

F. Relación entre la legislación sobre gestión de la identidad y la legislación sobre privacidad

En las transacciones de identidad con fines comerciales que conlleven la expedición o utilización de una credencial de identidad intervendrán con frecuencia algunos datos personales. En esos casos, la privacidad de esos datos personales puede ser importante.

Las leyes sobre privacidad suelen ocuparse de la protección de los datos personales en consonancia con el orden público pertinente. En consecuencia, el Grupo de Trabajo tal vez desee examinar la relación entre esas leyes y los sistemas de gestión de la identidad.

G. Relación entre la legislación sobre gestión de la identidad y la legislación sobre la seguridad de los datos

La seguridad de los datos reviste una importancia crítica para el funcionamiento correcto y la fiabilidad de las transacciones de identidad, tanto desde el punto de vista de la protección de la confidencialidad de los datos personales presentes en esas transacciones como para garantizar el funcionamiento correcto y la fiabilidad de las comunicaciones de credenciales que constituyen la propia transacción.

Las leyes de protección de datos se ocupan a menudo de la seguridad de los datos personales en consonancia con el orden público pertinente. Análogamente, otras leyes sobre la seguridad de los datos podrán hacer lo mismo con respecto a la protección de otros aspectos de las comunicaciones de transacciones de identidad. Por tanto, el Grupo de Trabajo tal vez desee estudiar la relación entre esas leyes y los sistemas de gestión de la identidad.

H. Relación en entre las normas de sistemas de base contractual y otra legislación

Como los sistemas de gestión de la identidad se regirán habitualmente por normas de sistemas de base contractual (es decir, marcos de confianza) convenidos por los participantes en esos sistemas, el Grupo de Trabajo tal vez desee analizar la relación entre esas normas y las leyes aplicables que no guarden relación directa con la identidad.

V. Temas sustantivos

A. Reconocimiento jurídico

El Grupo de Trabajo tal vez desee examinar el tema del reconocimiento jurídico de la información de identidad autenticada en una operación comercial. A ese respecto, el Grupo de Trabajo tal vez desee ocuparse de qué es el reconocimiento jurídico, qué es lo que trata de lograr y los requisitos para obtenerlo; quién otorga el reconocimiento jurídico; los fines para los que se otorga el reconocimiento jurídico; la relación entre el reconocimiento jurídico y las leyes que exigen alguna forma de identificación, como las que rigen la certificación por notario, la obligación de conocer al cliente, la lucha contra el blanqueo de dinero, el acceso a datos personales, y la forma, en su caso, de que el reconocimiento jurídico se aplique a la identidad de personas jurídicas, dispositivos u objetos digitales.

B. Reconocimiento transfronterizo mutuo

El concepto del reconocimiento mutuo es importante para facilitar la utilización de credenciales de identidad con fines comerciales, así como la confianza en esas credenciales, tanto en los distintos sistemas de identidad como a través de los límites jurisdiccionales.

Las cuestiones que el Grupo de Trabajo tal vez desee estudiar con respecto al tema del reconocimiento mutuo son numerosas. Algunas de las más obvias se refieren a ocuparse de: a) si debe existir o no el requisito de reconocer las credenciales; b) si existe el requisito de reconocer las credenciales, ¿quién debe estar obligado a reconocerlas?; c) si existe el requisito de reconocer las credenciales, ¿de qué parte deberían reconocerse las credenciales?; d) ¿cuál es la finalidad de ese reconocimiento mutuo?; e) ¿qué significa exactamente "reconocimiento mutuo"?; f) ¿qué características (es decir, niveles de garantía) deberían estar presentes para el reconocimiento mutuo?; g) ¿deberían existir límites en relación con el momento en que se aplica el reconocimiento mutuo?; y h) ¿debería aplicarse el reconocimiento mutuo a la identidad de personas jurídicas, dispositivos u objetos digitales?

C. Atribución de información de identidad a un sujeto

La atribución de información de identidad a un sujeto (para incluirla en una credencial de identidad) suele ser un elemento esencial de los sistemas de gestión de la identidad. Una cuestión fundamental que rige la atribución es el momento y las circunstancias en que los datos de identidad en una credencial han de atribuirse a un sujeto específico.

El Grupo de Trabajo tal vez desee examinar esa cuestión desde dos perspectivas. En primer lugar, ¿de qué forma debería garantizar un proveedor de identidad que la información que incluye en una credencial de identidad acerca de un sujeto efectivamente describe el sujeto nombrado en la credencial? En segundo lugar, cuando se utiliza una credencial de identidad, ¿de qué forma puede una parte que confía garantizar que la información en la credencial guarda relación con al sujeto que presenta dicha credencial?

D. Fiabilidad y atribución de acción, mensaje de datos o firma a un sujeto

Una cuestión fundamental para todos los participantes en un sistema de identidad es el momento y las circunstancias en que la confianza de una parte en una credencial de identidad es apropiada y razonable. El carácter razonable de la confianza de un parte puede afectar a una serie de cuestiones, por ejemplo, cuando se confía en una credencial de identidad errónea.

Por ejemplo, en el contexto de las firmas electrónicas, esa cuestión se abordó en el artículo 13 de la Ley Modelo sobre Comercio Electrónico.

E. Responsabilidad y adjudicación de riesgos

Las cuestiones de responsabilidad y adjudicación de riesgos son citadas con frecuencia como grandes obstáculos a la implantación de sistemas de identidad comerciales. Entre esas cuestiones figuran las siguientes: a) las preocupaciones de los proveedores de identidad y otros participantes en sistemas de identidad de que el riesgo de responsabilidad que se les adjudica de conformidad con la legislación vigente es improcedente o simplemente demasiado oneroso para permitirles proceder, así como b) las preocupaciones de los participantes en sistemas de identidad de que la ley es demasiado imprecisa, ambigua o poco clara para que puedan evaluar correctamente los riesgos que entraña su participación.

El Grupo de Trabajo tal vez desee plantearse si debería ocuparse de la cuestión de la responsabilidad y, de ser así, en relación con qué funciones del sistema de identidad y de qué forma. El Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior de la Unión Europea y la Ley de Gestión Electrónica de la Identidad del Estado de Virginia son ejemplos de instrumentos legislativos que se ocupan de la responsabilidad en el contexto de sistemas de gestión de la identidad.

F. Transparencia

Los procesos, procedimientos y tecnología empleados por un proveedor de identidad para expedir y validar credenciales de identidad pueden influir considerablemente en la fiabilidad de las transacciones de identidad en las que se utilicen esas credenciales. Así pues, puede ser importante que los demás participantes en un sistema de identidad entiendan cómo se ejecutan los citados procesos, procedimientos y tecnología para que estén en condiciones de realizar su propia evaluación de la fiabilidad de las transacciones de identidad consiguientes. A tal efecto, el Grupo de Trabajo tal vez desee examinar si existe o no un nivel adecuado de transparencia por parte de determinados participantes en un sistema de identidad. Análogamente, en caso de transgresión o exposición a un peligro en cualquiera de los procesos, procedimientos, tecnología, bases de datos o credenciales de identidad que una parte mantenga en el contexto de un sistema de identidad, el Grupo de Trabajo tal vez desee estudiar si debería divulgarse información sobre esa puesta en peligro.

En algunos casos, los requisitos de transparencia también han sido utilizados como elemento sustitutivo de la regulación que obliga a utilizar determinados procesos, procedimientos o tecnología. Un enfoque basado en la transparencia permite que las partes adopten sus propias decisiones sobre la fiabilidad en función de una información más completa.

G. Fiabilidad y niveles de garantía

En muchos sistemas de identidad se definen los denominados “niveles de garantía” o “niveles de seguridad” para ayudar a los participantes a responder a las preocupaciones relativas a la fiabilidad de las credenciales de identidad y las transacciones de identidad. Existen varios sistemas de niveles de garantía y suelen entrañar distintas gradaciones de garantía. Por ejemplo, en su Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, la UE define tres niveles de seguridad (denominados “bajo”, “alto” y “sustancial”), mientras que en los Estados Unidos y otros países se emplean cuatro niveles de garantía.

El Grupo de Trabajo tal vez desee plantearse la mejor forma de facilitar la confianza de los participantes en un sistema de identidad. Si bien es cierto que el concepto de niveles de garantía es de uso común, puede que el Grupo de Trabajo desee también estudiar otros mecanismos como la transparencia por mandato, la certificación por terceros u otros enfoques que puedan emplearse para ayudar a facilitar la confianza.